RODO DLA BIBLIOTEK

Kodeks postępowania wspierający we właściwym stosowaniu RODO

SBP
STOWARZYSZENIE
BIBLIOTEKARZY
POLSKICH

Autorzy kodeksu
dr hab. Jarosław Czerw (podrozdziały nr 5.2, 9.4, 9.12)
Sylwia Czub-Kiełczewska (podrozdziały nr 1.1, 1.3, 1.4, 2.7, 3.6, 4.1, 4.4, 7.5, 9.1-9.3, 9.7, 9.9, 9.13, 11.1, 11.2, 11.5, 11.6)
Piotr Kaczmarek (podrozdziały nr 2.5, 2.6, 3.4, 4.3, 5.3, 9.8)
Dorota Mika (podrozdziały nr 2.3, 2.4, 3.1, 3.2, 4.2, 9.10, 9.11, 11.3)
Marta Rejner (podrozdziały nr 6.1-6.4, 6.6, 10.1)
Mariusz Warkoczyński (podrozdziały nr 7.1-7.4)
dr Łukasz Wojciechowski (podrozdziały nr 1.2, 2.1, 2.2., 3.3, 3.5, 5.1, 6.5, 8.1-8.4, 10.3)
Michał Zajączkowski (podrozdziały nr 9.5, 9.6, 10.2)

Redakcja kodeksu
Sylwia Czub-Kiełczewska (rozdziały nr 1, 4,7, 9, 11)
dr Łukasz Wojciechowski (rozdziały nr 2, 3, 5, 6, 8, 10)

Redakcja techniczna
Marta Lach

Projekt graficzny, skład i łamanie
Ewa Majewska

Konsultanci	**Adres**
Monika Bogusz	Powiatowa Biblioteka Publiczna w Łęcznej
Izabela Chruszcz	Dolnośląska Biblioteka Pedagogiczna we Wrocławiu
Monika Rejdych	Miejska Biblioteka Publiczna w Jaworznie
Dariusz Dylewski	Wojewódzka i Miejska Biblioteka Publiczna w Bydgoszczy
Anita Fal	Gminna Biblioteka Publiczna w Krościenku Wyżnym
Paweł Soczek	Wojewódzka Biblioteka Publiczna w Krakowie
Beata Zych	Pedagogiczna Biblioteka Wojewódzka w Warszawie
Wojciech Piasecki	Wojewódzka i Miejska Biblioteka Publiczna w Gdańsku
Maciej Wara Wąsowski	Biblioteka Miejska w Łodzi

ISBN: 978-83-65741-45-5

Wydawnictwo Naukowe i Edukacyjne Stowarzyszenia Bibliotekarzy Polskich
00-335 Warszawa, ul. Konopczyńskiego 5/7 tel. (22) 827-52-96
Warszawa 2020. Wyd. I.
www.sbp.pl; wydawnictwo@sbp.pl, biuro@sbp.pl

Spis treści

1 DLACZEGO POWSTAŁ KODEKS

1.1. Cel powstania Kodeksu i zasady jego monitorowania.

I. Cel powstania Kodeksu dla bibliotek.

Kodeks dla bibliotek to inicjatywa podjęta przez specjalistów w zakresie ochrony danych osobowych działających na rzecz bibliotek oraz Stowarzyszenia Bibliotekarzy Polskich [SBP], który powstał w celu zapewnienia merytorycznego i praktycznego wsparcia bibliotek, jako administratorów, w zapewnieniu prawidłowego i skutecznego stosowania przepisów o ochronie danych osobowych. Zawartość Kodeksu była tworzona i konsultowana ze wsparciem środowiska bibliotekarzy. Większość autorów to osoby pracujące lub stale współpracujące z instytucjami kultury, są to także specjaliści w dziedzinie stosowania przepisów o ochronie danych osobowych. Niniejszy Kodeks został opracowany na podstawie przepisów art. 40 RODO.

Stosowanie niniejszego Kodeksu nie zwalnia administratora ze śledzenia i wdrażania zmian, wynikających z nowelizacji powszechnie obowiązującego prawa, orzecznictwa, czy wytycznych organu nadzorczego. Już na etapie powstawania Kodeksu niezbędne były aktualizacje części podrozdziałów ze względu na zmieniające się przepisy prawa, wobec tego administrator stosujący niniejszy Kodeks musi brać pod uwagę konieczność weryfikacji przekazanych zapisów. Kodeks jest skierowany do bibliotek publicznych, w tym działających w ramach ośrodków kultury, pedagogicznych oraz wojskowych. Podmiotowy zakres stosowania Kodeksu wynika z trwających prac nad wytycznymi dla bibliotek będących w strukturach innych podmiotów, a także przeprowadzonych przez SBP konsultacji. Autorzy uwzględnili różnice wynikające z przetwarzania danych w bibliotekach będących odrębnymi jednostkami, jak i działających w ramach innych jednostek. Przyjęcie i stosowanie niniejszego Kodeksu ma pomóc kierownictwu biblioteki zapewnić prawidłowe i skuteczne stosowanie przepisów o ochronie danych osobowych, ze szczególnym uwzględnieniem specyfiki procesów bibliotecznych.

II. Zatwierdzenie Kodeksu przez organ nadzorczy.

Niniejszy Kodeks został upubliczniony, jako poradnik i do momentu zatwierdzenia i upublicznienia jego treści przez Prezesa UODO, zgodnie z art. 40 ust. 6 RODO, jego przyjęcie do stosowania w bibliotece nie będzie rozumiane jako stosowanie zatwierdzonego kodeksu postępowania, zgodnie z art. 40 ust. 3 RODO. Dyrektor biblioteki może niezależnie od powyższego, przyjąć do stosowania wytyczne wskazane w niniejszym Kodeksie, traktując je jako dobrą praktykę.

Treść Kodeksu przed przedłożeniem do zatwierdzenia Prezesowi UODO była konsultowana ze środowiskiem bibliotekarzy. Na etapie powstawania Kodeksu dokonano wyboru autorów wśród

osób ściśle związanych z działalnością bibliotek, zostali także wytypowani główni eksperci, będący pracownikami bibliotek. Na etapie tworzenia treści kodeksu, autorzy zadawali pytania ekspertom, w celu zasięgnięcia ich opinii, także w zakresie przyjętych już praktyk w zakresie stosowania przepisów RODO. Ostateczna treść kodeksu podlegała konsultacjom z branżą bibliotekarską, które były koordynowane przez SBP.

III. Przyjęcie zatwierdzonego Kodeksu do stosowania.

Po zatwierdzeniu ostatecznej wersji Kodeksu przez Prezesa UODO, przyjęcie do stosowania w bibliotece zatwierdzonego kodeksu postępowania powinno odbyć się na podstawie zarządzenia dyrektora biblioteki lub podmiotu, w strukturach którego działa biblioteka. Kodeks powinien dotyczyć wszystkich pracowników i współpracowników biblioteki, bez wyjątku, a także odnosić się do wszystkich lokalizacji, w których przetwarzane są dane osobowe, dla których administratorem jest biblioteka.

IV. Mechanizmy pozwalające monitorowanie przestrzegania przepisów Kodeksu.

Monitorowaniem przestrzegania Kodeksu postępowania na mocy art. 40 przez bibliotekę może się zajmować podmiot, który dysponuje odpowiednim poziomem wiedzy fachowej w dziedzinie będącej przedmiotem Kodeksu i został akredytowany w tym celu przez Prezesa UODO. Stowarzyszenie Bibliotekarzy Polskich opublikuje na swojej stronie dane podmiotów, które otrzymały niezbędną akredytację w celu monitorowania zgodności przetwarzania z zasadami określonymi w Kodeksie.

Zgodnie z art. 41 ust. 6 RODO podmioty publiczne nie mają obowiązku przechodzenia przez proces monitorowania Kodeksu, o którym mowa w art. 41 RODO. Należy jednak podkreślić, że powołany w bibliotece IOD powinien uwzględnić monitorowanie przestrzegania przyjętego Kodeksu w swoim planie audytów.

V. Zmiany i aktualizacje Kodeksu.

Biorąc pod uwagę, że przepisy prawa oraz praktyki stosowania przepisów RODO mogą ulegać szybkim zmianom, inicjatorzy i autorzy powstania Kodeksu będą publikować na dedykowanej stronie internetowej nieoficjalne wytyczne w zakresie dostosowania stosowania Kodeksu do wskazanych zmian, a także przedłożą zaktualizowaną treść Kodeksu Prezesowi UODO w celu zatwierdzenia zmian. Wszystkie aktualizacje Kodeksu będą publikowane na dedykowanej stronie, a także przez Prezesa UODO.

VI. Działalność edukacyjna.

Stowarzyszenie Bibliotekarzy Polskich mając na uwadze konieczność wspierania branży bibliotecznej w dostosowaniu procesów bibliotecznych do zasad zawartych w Kodeksie, deklaruje wsparcie w zakresie prowadzonych okresowo szkoleń, a także publikowania wyjaśnień ekspertów w zakresie sposobu realizacji poszczególnych postanowień Kodeksu. SBP będzie przyjmować także wszelkie uwagi i wnioski odnoszące się do treści Kodeksu, a także koordynować jego aktualizacje.

1.2. Znaczenie RODO dla bibliotek oraz ich użytkowników.

Biblioteki to instytucje, które mają szczególne znaczenie dla rozwoju społeczeństwa, promocji wiedzy, nauki, jak również edukacji w zakresie kultury. Społeczność lokalna może nie tylko wypożyczać książki, ale też coraz częściej korzystać z bogatej oferty wydarzeń, m.in. warsztatów, spotkań autorskich, wystaw i wielu innych przedsięwzięć. Biblioteki to jednocześnie instytucje publiczne, które funkcjonują także w wymiarze administracyjnym, realizując obowiązki prawne wynikające z szerokiego spektrum aktów normatywnych. Tak jak w przypadku innych podmiotów administracji publicznej, realizacja celów bibliotek wiąże się bowiem z zabezpieczeniem odpowiednich środków finansowych, utrzymaniem i ogrzewaniem budynków, zatrudnianiem pracowników i wieloma innymi czynnościami. Jednym z priorytetów funkcjonowania wszystkich instytucji publicznych jest zapewnienie bezpieczeństwa swoim użytkownikom. Bezpieczeństwo to ma szeroki wymiar i z jednej strony odnosi się do tego, żeby nikomu nie stała się fizyczna krzywda podczas przebywania w siedzibie instytucji. Z drugiej strony konieczne jest podejmowanie działań, które zapobiegają popełnianiu przestępstw na szkodę użytkowników, które zostają dokonane w konsekwencji korzystania z usług instytucji. Jednocześnie, osoby fizyczne korzystające z usług instytucji publicznych mają prawo do ochrony swojej prywatności. Z punktu widzenia bibliotek ma to tym bardziej istotne znaczenie, że dla wielu użytkowników są one instytucjami zaufania publicznego. W realizacji praw i prewencji zagrożeń, które odnoszą się do osób korzystających z bibliotek, ale również ich pracowników, priorytetowe znaczenie ma system ochrony danych osobowych. Jest on konsekwentnie budowany w Polsce od 30 kwietnia 1998 r., kiedy weszła w życie nieobowiązująca już ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych.

Warto podkreślić, że ochrona danych osobowych jest skomplikowaną materią, a optymalne rozwiązania w tym zakresie, zarówno w wymiarze prawnym, jak i praktycznym, są w dalszym ciągu wypracowywane nie tylko w Polsce, ale także w innych państwach na wszystkich kontynentach. Z jednej strony badana jest efektywność przyjętych rozwiązań, z drugiej konieczne jest systematyczne wypracowywanie nowych, z uwagi na zmieniającą się rzeczywistość. Stąd bardzo duże znaczenie z punktu widzenia budowania systemu ochrony danych osobowych w Polsce i innych państwach Unii Europejskiej miało opracowanie RODO i poddanie tego aktu prawnego procedurom legislacyjnym, których efektem jest to, że RODO od 25 maja 2018 r. obowiązuje bezwzględnie we wszystkich państwach Unii Europejskiej. Dla kadry kierowniczej i pracowników bibliotek RODO oznacza przede wszystkim:

- konieczność zapoznania się z przepisami RODO i stosowanie bezpośrednio tego aktu prawnego,
- otrzymanie zbioru spójnych procedur w postaci aktu prawnego z obszerną preambułą, w której wyjaśnione są intencje twórców poszczególnych przepisów RODO (propozycje szczegółowych rozwiązań w zakresie stosowania przepisów w praktyce zostały przedstawione w niniejszym Kodeksie),
- konieczność aktualizacji procedur wewnętrznych oraz przegląd umów zawartych z innymi podmiotami pod kątem ewentualnego powierzania danych osobowych,
- obowiązek realizacji znacząco rozbudowanych, na mocy nowych przepisów, praw osób fizycznych, np. prawa do bycia zapomnianym,
- konieczność wypełniania obowiązku informacyjnego wobec wszystkich osób fizycznych pracujących w bibliotece lub korzystających z jej usług (dotyczy to także strony internetowej oraz OPAC biblioteki),
- konieczność przeprowadzania analizy ryzyka w związku z przetwarzanymi danymi osobowymi,
- potencjalną współpracę z nowym organem – Prezesem Urzędu Ochrony Danych Osobowych (dawniej Generalny Inspektor Ochrony Danych Osobowych),

- obowiązek zgłaszania do Prezesa UODO naruszeń bezpieczeństwa danych osobowych w ciągu 72 godzin od momentu powzięcia informacji o naruszeniu, jeżeli istnieje ryzyko naruszenia praw lub wolności osób fizycznych,
- obowiązek wyznaczenia Inspektora Ochrony Danych i współpracy z osobą pełniącą tę funkcję,
- obowiązek regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania,
- obowiązek podejmowania innych działań zgodnie z przepisami RODO, opisanych w niniejszym Kodeksie.

Wejście w życie przepisów RODO wiąże się z dodatkowymi obowiązkami dla biblioteki, jednak ich systematyczne i staranne realizowanie bez wątpienia przyczyni się do zwiększenia bezpieczeństwa danych osobowych osób fizycznych, przetwarzanych w ramach funkcjonowania biblioteki. Dla użytkowników biblioteki RODO oznacza przede wszystkim zwiększenie bezpieczeństwa ich danych osobowych, co wynika z dwóch czynników. Pierwszy to obowiązek prawny nałożony na bibliotekę w zakresie realizacji przepisów RODO. Użytkownik w związku z tym dostaje możliwość uzyskania informacji na temat zakresu jego danych osobowych, jakie są przetwarzane przez instytucję. Ponadto, w RODO został usankcjonowany szeroki katalog praw osób fizycznych, które obowiązują także w przypadku korzystania z biblioteki (zostały opisane w niniejszym Kodeksie). Użytkownicy mają też możliwość skontaktowania się z IOD w bibliotece i poinformowania go o nieprawidłowościach. Mogą także bezpłatnie złożyć skargę do Prezesa UODO. Równie istotne znaczenie ma także drugi czynnik – wzrost świadomości kadry kierowniczej i pracowników biblioteki w zakresie ochrony danych osobowych. Samo wejście w życie przepisów RODO wiązało się bowiem z szeroką dyskusją na ten temat, jak również ukazaniem się wielu wartościowych artykułów i innych publikacji. Wielu pracowników bibliotek już skorzystało, lub skorzysta w najbliższej przyszłości z dostępnych wartościowych szkoleń w zakresie ochrony danych osobowych. Przy odpowiednim podejściu do przepisów RODO – sumiennym, ale także racjonalnym, na wejściu w życie rozporządzenia skorzystają zarówno biblioteki, jak i osoby korzystające z ich usług.

1.3. Wykaz aktów prawnych.

Niniejszy Kodeks został opracowany w oparciu o wskazane poniżej przepisy powszechnie obowiązującego prawa. Treści Kodeksu zostały opracowane i są zgodne ze stanem prawnym na dzień 30.09.2019 r. Poniżej wskazano akty prawne wykorzystane w Kodeksie, a także skróty, którymi posługiwali się autorzy przywołując te akty.

MIĘDZYNARODOWE PRZEPISY PRAWA:

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (Dz. Urz. WE L 281 z 23.11.1995) – **dalej Dyrektywa 95/46/WE.**

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dn. 27-04-2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.) – **dalej RODO.**

Powszechna Deklaracja Praw Człowieka (przyjęta i proklamowana rezolucja Zgromadzenia Ogólnego ONZ 217 A (III) w dniu 10 grudnia 1948 r.).

Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (Dz.U. 1977 nr 38 poz. 167) – **dalej Międzynarodowy Pakt Praw Obywatelskich i Politycznych.**

Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz.U. 1993 nr 61 poz. 284) – **dalej Europejska Konwencja Praw Człowieka.**

Karta Praw Podstawowych Unii Europejskiej (Dz. Urz. UE C 326/391 z 26.10.2012 r.) – **dalej Karta Praw Podstawowych UE.**

KRAJOWE PRZEPISY PRAWA:

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r. (Dz.U. 1997 nr 78 poz. 483 z późn. zm.) – **dalej Konstytucja RP.**

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2019 poz. 1781 z późn. zm.) – **dalej Ustawa ODO.**

Ustawa o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), (Dz.U. 2019 poz. 730 z późn. zm.) – **dalej Ustawa wdrażająca RODO.**

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (uchylona 25.05.2018 r.) – **dalej stara Ustawa ODO.**

Ustawa z dnia 27 czerwca 1997 r. o bibliotekach (Dz.U. 2019 poz. 1479 z późn. zm.) – **dalej ustawa o bibliotekach.**

Ustawa z dnia 25 października 1991 r. o organizowaniu i prowadzeniu działalności kulturalnej (Dz. U. z 2018 r. poz. 1983 z późń. zm) – **dalej ustawa o organizowaniu u prowadzeniu działalności kulturalnej.**

Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz.U. 2019 poz. 1040 z późn. zm.) – **dalej Kodeks pracy lub KP.**

Ustawa z dnia 23 kwietnia 1964 r. - Kodeks cywilny (Dz.U. 2019 poz. 1145 z późn. zm.) – **dalej Kodeks cywilny lub KC.**

Ustawa z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (Dz.U. 2019 poz. 1460 z późn. zm.) – **dalej Kodeks postępowania cywilnego lub KPC.**

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (tekst jedn. Dz.U. z 2018 r. poz. 1600 z późn. zm.) – **dalej Kodeks karny.**

Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz.U. z 2018 r. poz. 1987 z późn. zm.) – **dalej Kodeks postępowania karnego lub KPR.**

Ustawa z dnia 25 czerwca 1999 r. o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa (Dz.U. 2019 poz. 645 z późn. zm.) – **dalej ustawa o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa.**

Ustawa z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych (Dz.U. 2019 poz. 1387 z późń.) – **dalej ustawa o podatku dochodowym.**

Rozporządzenie Rady Ministrów z dnia 19 grudnia 1992 r. w sprawie pracowniczych kas zapomogowo-pożyczkowych oraz spółdzielczych kas oszczędnościowo-kredytowych w zakładach pracy (Dz.U. 1992 nr 100 poz. 502, z późń. zm.) – dalej **rozporządzenie w sprawie pracowniczych kas zapomogowo-pożyczkowych oraz spółdzielczych kas oszczędnościowo-kredytowych w zakładach pracy.**

Ustawa z dnia 4 marca 1994 r. o zakładowym funduszu świadczeń socjalnych (Dz.U. 2019 poz. 1352 z późn. zm.) – **dalej ustawa o ZFŚS.**

Ustawa z dnia 23 maja 1991 r. o związkach zawodowych (Dz.U. 2019 poz. 263, z pożn. zm.) – **dalej ustawa o związkach zawodowych.**

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. 2019 poz. 123 z późn. zm.) – **dalej UŚUDE.**

Ustawa z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz. U. z 2019 r. poz. 649 z późn. zm.) – **dalej ustawa o statystyce publicznej.**

Ustawa z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz.U. 2018 poz. 1668 z późn. zm.) – **dalej Prawo o szkolnictwie wyższym i nauce.**

Ustawa z dnia 17 lipca 2009 r. o praktykach absolwenckich (Dz.U. 2018 poz. 1244 z późn. zm.) – **dalej ustawa o praktykach absolwenckich.**

Ustawa z dnia 14 grudnia 2016 r. – Prawo oświatowe (Dz.U. 2019 poz. 1148 z późn. zm.) – **dalej Prawo oświatowe.**

Ustawa z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy (Dz.U. 2019 poz. 1482 z późń. zm.) – **dalej ustawa o promocji zatrudnienia i instytucjach rynku pracy.**

Rozporządzenie Ministra Edukacji Narodowej z dnia 24 sierpnia 2017 r. w sprawie praktycznej nauki zawodu (Dz.U. 2017 poz. 1644 z późń. zm.) – **dalej rozporządzenie w sprawie praktycznej nauki zawodu.**

Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. 2019 poz. 1231 z późn. zm.) – **dalej Prawo autorskie.**

Rozporządzenie Ministra Zdrowia i Opieki Społecznej w sprawie przeprowadzania badań lekarskich pracowników, zakresu profilaktycznej opieki zdrowotnej nad pracownikami oraz orzeczeń lekarskich wydawanych do celów przewidzianych w Kodeksie pracy (Dz.U. 2016 poz. 2067 z późn. zm.) – **dalej rozporządzenie w sprawie przeprowadzania badań lekarskich pracowników, zakresu profilaktycznej opieki zdrowotnej nad pracownikami oraz orzeczeń lekarskich wydawanych do celów przewidzianych w Kodeksie pracy.**

Ustawa z dnia 30 października 2002 r. o ubezpieczeniu społecznym z tytułu wypadków przy pracy i chorób zawodowych (Dz.U. 2019 poz. 1205 z późn. zm.) – **dalej ustawa o ubezpieczeniu społecznym z tytułu wypadków przy pracy i chorób zawodowych.**

Ustawa z dnia 30 października 2002 r. o ubezpieczeniu społecznym z tytułu wypadków przy pracy i chorób zawodowych (Dz.U. 2019 poz. 1205 z późn. zm.) – **dalej ustawa o ubezpieczeniu społecznym z tytułu wypadków przy pracy i chorób zawodowych.**

Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 19 grudnia 2018 r. w sprawie szczegółowych zasad orzekania o stałym lub długotrwałym uszczerbku na zdrowiu, trybu postępowania przy ustalaniu tego uszczerbku oraz postępowania i wypłatę jednorazowego odszkodowania (Dz.U. 2018 poz. 2403 z późn. zm.) – **dalej rozporządzenie w sprawie szczegółowych zasad orzekania o stałym lub długotrwałym uszczerbku na zdrowiu, trybu postępowania przy ustalaniu tego uszczerbku oraz postępowania i wypłatę jednorazowego odszkodowania.**

Rozporządzenie Rady Ministrów z dnia 1 lipca 2009 r. w sprawie ustalenia okoliczności i przyczyn wypadków przy pracy (Dz.U. z 2009 r., nr 105. poz.870 z późn. zm.) – **dalej rozporządzenie w sprawie ustalenia okoliczności i przyczyn wypadków przy pracy.**

Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz.U. z 2019 r. poz. 161 z późń. zm.) – **dalej ustawa o Policji.**

Ustawa z dnia 28 stycznia 2016 r. Prawo o prokuraturze (Dz.U. 2019 r. poz. 740 z późń. zm.) – **dalej prawo o prokuraturze.**

Ustawa z dnia 22 marca 2018 r. o komornikach sądowych (Dz.U. z 2018 r. poz. 771 z późn. zm.) – **dalej ustawa o komornikach sądowych.**

Ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz.U. z 2019 r. poz 300 z późn. zm.) – **dalej ustawa o systemie ubezpieczeń społecznych.**

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (uchylone dn. 06.02.2019 r.) – **dalej rozporządzenie w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.**

Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U. 2019 poz. 869 z późn. zm.) – **dalej ustawa o finansach publicznych.**

Ustawa z dnia 19 listopada 2009 r. o grach hazardowych (Dz.U. 2019 poz. 847 z poźn. zm.) – **dalej ustawa o grach hazardowych.**

Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U z 2019 r., poz. 506 z późn. zm.) – **dalej ustawa o samorządzie gminnym.**

Ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz.U. z 2019 r., poz. 511 z późn. zm.) – **dalej ustawa o o samorządzie powiatowym.**

Ustawa z 7 października 1992 r. o regionalnych izbach obrachunkowych (Dz.U. z 2016 r. poz. 561 z późn. zm.) – **dalej ustawa o regionalnych izbach obrachunkowych.**

Ustawa z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2019 r. poz. 489, z późn. zm.) – **dalej ustawa o NIK.**

Ustawa z dnia 13 kwietnia 2007 r. o Państwowej Inspekcji Pracy (Dz.U. 2019 poz. 1251, z późn. zm.) – **dalej ustawa o PIP.**

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2019 poz. 700 z późn. zm.) – **dalej ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne.**

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2017 poz. 2247 z późn. zm.) – **dalej Krajowe Ramy Interoperacyjności lub KRI.**

LITERATURA WYKORZYSTANA W KODEKSIE

T. Banyś, P. Biały, T. Błoński, P. Glen, M. Kwiatkowska-Cylke, J. Łuczak, Ł. Onysyk, A. Kręcisz-Sarna, M. Sarna, J. Sobczak, A. Stępień, *RODO Przewodnik po kluczowych zmianach*, Wyd. Wiedza i Praktyka, Warszawa 2018.

A. Kaczmarek, M. Młotkiewicz, A. Łapińska, A. Miłocha, M. Mazur, *Jak rozumieć podejście oparte na ryzyku? Poradnik RODO. Podejście oparte na ryzyku*. Część 1, https://uodo.gov.pl/data/filemanager_pl/706.pdf [dostęp 30.09.2019].

A. Kaczmarek, M. Młotkiewicz, A. Łapińska, A. Miłocha, M. Mazur, *Jak stosować podejście oparte na ryzyku? Poradnik RODO. Podejście oparte na ryzyku*. Część 2, https://uodo.gov.pl/data/filemanager_pl/707.pdf [dostęp 30.09.2019].

Ochrona danych osobowych w szkołach i placówkach oświatowych – poradnik, https://uodo.gov.pl/pl/p/ochrona-danych-osobowych-w-szkolach-i-placowkach-oswiatowych-poradnik [dostęp 30.09.2019].

1.4. Słownik pojęć oraz skrótów użytych w Kodeksie.

ADO – administrator danych osobowych.

Czytelnik – osoba zarejestrowana w bibliotece, która zaakceptowała regulamin korzystania z zasobów bibliotecznych oraz podpisała kartę zobowiązania.

DKK – Dyskusyjne Kluby Książki.
DPIA – ocena skutków
EROD – Europejska Rada Ochrony Danych (dawniej Grupa robocza art. 29).
GIODO – dawna nazwa organu nadzorczego, tzn. Prezesa UODO.
Grupa robocza art. 29 – dawna nazwa EROD.
IOD – inspektor ochrony danych.
OPAC – aplikacja lub system umożliwiający przeglądanie zasobów bibliotecznych przez Internet. Niektóre OPAC oferują dodatkowe funkcje dla zarejestrowanych użytkowników.
PKZP – Pracownicza Kasa Zapomogowo Pożyczkowa.
Prezes UODO – Prezes Urzędu Ochrony Danych Osobowych będący polskim organem nadzorczym.
UODO – Urząd Ochrony Danych Osobowych, jednostka pomocnicza organu nadzorczego.
Użytkownik – w niniejszym Kodeksie określenie używane w dwóch znaczeniach: 1) osoby, korzystającej z oferty bibliotecznej, niekoniecznie zarejestrowanego czytelnika 2) użytkownik systemu informatycznego, który otrzymał stosowne uprawnienia od administratora.
SZBI – System Zarządzania Bezpieczeństwem Informacji.
ZFŚS – Zakładowy Fundusz Świadczeń Socjalnych.

2 BIBLIOTEKA JAKO PODMIOT PRZETWARZAJĄCY DANE OSOBOWE

2.1. Biblioteka jako administrator danych osobowych.

Przed rozpoczęciem przetwarzania danych osobowych i podejmowania działań zmierzających do ochrony danych osobowych należy zrozumieć na czym polega rola biblioteki jako administratora danych osobowych. W obowiązujących i już nieobowiązujących aktach normatywnych regulujących zagadnienia związane z ochroną danych osobowych, w książkach na ten temat, blogach i innych stronach internetowych można znaleźć co najmniej trzy określenia:

- administrator,
- administrator danych,
- administrator danych osobowych.

W przypadku tego ostatniego określenia bardzo często używany jest skrót „ADO". Wskazane określenia należy traktować jako synonimy, które oznaczają dokładnie to samo. Definicja „administratora danych" znana jest przede wszystkim z nieobowiązującej już ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, którą biblioteki stosowały przez ponad dwadzieścia lat (od 30 kwietnia 1998 r. do 25 maja 2018 r.). Zgodnie z nią jest to organ, jednostka organizacyjna, podmiot lub osoba, decydujące o celach i środkach przetwarzania danych osobowych. Warto pamiętać, że definicje w ustawie z 1997 r. były wzorowane na dyrektywie 95/46/WE. W definicji „administratora danych" tam zawartej również położono nacisk na to, że ADO jest ten, kto samodzielnie lub wspólnie z innymi podmiotami określa cele i sposoby przetwarzania danych. RODO jest kontynuacją wskazanej dyrektywy i po wejściu w życie RODO w praktyce nic nie zmieniono jeśli chodzi o ADO. Przepisy prawa są więc jednoznaczne – zarówno przed reformą systemu ochrony danych osobowych, jak również po wejściu w życie RODO biblioteka jest administratorem (danych osobowych) – ADO.

Takie kategoryczne stwierdzenie jest o tyle istotne, że w przypadku niektórych podmiotów administracji publicznej pojawiają się trudności z precyzyjnym wskazaniem ADO. Przykładem mogą być urzędy wojewódzkie. Niektórzy zastanawiają się czy administratorem danych osobowych jest wojewoda, dyrektor generalny czy sam urząd, skoro ustawodawca przydzielił im różne kompetencje szczegółowe, które oznaczają decydowanie o celach i środkach przetwarzania danych. Przykładów wątpliwości w tym zakresie jest oczywiście znacznie więcej. Niektórzy zastanawiają się, dlaczego dany podmiot jest administratorem danych, jeżeli wykonuje wyłącznie zadania wskazane precyzyjnie w ustawie i w związku z tym nie decyduje o celach i środkach, mając je po prostu narzucone. Takie dywagacje warto jednak zostawić pasjonatom ochrony danych osobowych, którzy prowadzą wielowątkowe dyskusje na zrzeszających ich grupach i forach w Internecie. W przypadku bibliotek ta kwestia jest klarowna, chociaż też pojawiają się wątpliwości, o których warto wspomnieć. Niektórzy

pracownicy zastanawiają się, dlaczego ADO w przypadku biblioteki nie jest jej dyrektor. Jest to bowiem osoba, która odpowiada za funkcjonowanie instytucji i decyduje o kluczowych kwestiach. Jest to jednak błędne postawienie sprawy, ponieważ dyrektor nie jest w stanie kontrolować każdej czynności związanej z przetwarzaniem danych osobowych. Wiele decyzji muszą podejmować spontanicznie i intuicyjnie pracownicy, nawet jeśli nie podejmują strategicznych decyzji na temat kierunków rozwoju biblioteki. Można więc w dużym uproszczeniu porównać kwestię ADO do budowli składającej się z wielu elementów. Nawet jeśli większość z nich jest układanych przez dyrektora, to każdy z pracowników również dokłada swoje elementy, które docelowo składają się na powstałą konstrukcję. Nie bez znaczenia jest też to, że dyrektorzy bibliotek się zmieniają, np. przechodząc na emeryturę. Instytucja funkcjonuje nadal, a decyzje zarówno aktualnego kierownictwa, jak i poprzedników mają realny wpływ na to, jak przetwarzane są dane osobowe.

Jeżeli ktoś chciałby odpowiedzieć krótko na pytanie, co to znaczy, że biblioteka jest ADO, będzie to zadanie bardzo trudne. W preambule i przepisach RODO określenie „administrator" występuje prawie pięćset razy. Bez wątpienia bycie ADO w przypadku biblioteki oznacza, że instytucja musi stosować przepisy RODO i przepisy Ustawy ODO. Stosowanie tych regulacji będzie w praktyce oznaczało przede wszystkim zapewnienie realizacji wielu praw osób fizycznych, których dane dotyczą. Obowiązkowe stało się także zgłaszanie naruszeń ochrony danych osobowych do Prezesa UODO. Samo przetwarzanie musi odbywać się zgodnie z zasadami wskazanymi w RODO i zawsze tylko wtedy, gdy istnieje legalna przesłanka przetwarzania. Wszystkie istotne i potrzebne w codziennym funkcjonowaniu biblioteki aspekty bycia ADO oraz prawidłowego i bezpiecznego przetwarzania danych osobowych zostały omówione w kolejnych rozdziałach i podrozdziałach niniejszego Kodeksu.

2.2. Status biblioteki w strukturze innego podmiotu.

Jeżeli biblioteka funkcjonuje jako samodzielny podmiot, mający nadane numery identyfikacyjne NIP i REGON to opisana w podrozdziale 2.1. kwestia bycia ADO nie powinna budzić wątpliwości. Istnieją jednak biblioteki, które nie są samodzielnymi jednostkami. Funkcjonują np. w strukturze szkoły, uczelni wyższej, jednostki wojskowej lub innych podmiotów. W takich przypadkach również należy stosować przepisy RODO, mając jednak świadomość przynależności do większej struktury.

Przede wszystkim w takiej sytuacji biblioteka nie jest ADO. Administratorem jest natomiast cały podmiot, w strukturę którego wchodzi biblioteka. Np. Biblioteka Uniwersytetu Marii Curie-Skłodowskiej w Lublinie nie jest ADO. Jest nim Uniwersytet Marii Curie-Skłodowskiej w Lublinie. Podobnie biblioteka wojskowa nie ma statusu administratora dla danych czytelników, gdyż działa w strukturach jednostki wojskowej, czyli faktycznego administratora Warto podkreślić, że w przypadku wskazanych podmiotów, przez administratora należy rozumieć jednostkę organizacyjną, w strukturach której działa biblioteka, a nie kierownika, dowódcę, czy dyrektora tej jednostki. Nie oznacza to jednak, że biblioteka nie musi chronić danych osobowych zgodnie z uregulowaniami prawnymi RODO. Pracownicy i kadra kierownicza takich bibliotek muszą współpracować w tym zakresie z pozostałymi jednostkami organizacyjnymi, ścisłym kierownictwem instytucji oraz IOD. Odbywa się to na kilku płaszczyznach poprzez:

- zapewnienie, aby dokumentacja ochrony danych osobowych – procedury, rejestr czynności przetwarzania, rejestr kategorii czynności przetwarzania, analiza ryzyka i inne dokumenty odnosiły się także do specyficznych procesów przetwarzania danych osobowych charakterystycznych dla bibliotek,
- zapewnienie, aby IOD nie lekceważył lub nie bagatelizował roli biblioteki w strukturze całego

podmiotu – wszystkimi czynnościami jakie wykonuje powinien również objąć bibliotekę i być w stanie udzielić wskazówek odnośnie przetwarzania danych osobowych czytelników oraz użytkowników,

- zagwarantowanie pracownikom biblioteki pozostającej w strukturze innego podmiotu dostępu do wartościowych szkoleń i systematycznego rozwiewania ich wątpliwości na temat bezpiecznego przetwarzania danych osobowych – władze podmiotu, w strukturze którego znajduje się biblioteka powinny wygospodarować na to środki finansowe, bądź też zaangażować do realizacji tego zadania IOD,
- należyte przygotowanie do realizowania praw osób fizycznych, których dane dotyczą pracowników biblioteki pozostającej w strukturze innego podmiotu – udzielenia im precyzyjnej informacji w jaki sposób mogą realizować swoje prawa i jak została zorganizowana ochrona danych osobowych w związku z tym, że biblioteka pozostaje częścią większej struktury,
- przećwiczenie niektórych procedury ze szczególnym uwzględnieniem reagowania w sytuacjach kryzysowych, zanim takie sytuacje wydarzą się naprawdę – np. przeprowadzenie z pracownikami symulacji postępowania w przypadku naruszenia bezpieczeństwa ochrony danych osobowych, które realnie grozi naruszeniem praw i wolności osób fizycznych i kwalifikuje się do zgłoszenia w ciągu 72 godzin do Prezesa UODO (pracownicy muszą wiedzieć do kogo powinni się w takiej sytuacji zgłosić, również w sytuacji, w której chwilowo nie ma kontaktu z IOD).

2.3. Czym są dane osobowe i na czym polega ich przetwarzanie?

Za dane osobowe uważa się wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Zgodnie z art. 4 pkt 1 RODO dane osobowe „oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej".

W RODO wyznaczono zakres przedmiotowy, w jakim rozporządzenie ma zastosowanie. Stosuje się je wyłącznie do ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych. Przyjmuje się, że do identyfikacji osoby fizycznej wystarczą tzw. „dane zwykłe" tzn. dane umożliwiające określenie konkretnej osoby fizycznej, których pozyskanie nie wymaga nakładu czasu, środków ani kosztów, do których zalicza się w szczególności: imię, nazwisko, adres zamieszkania lub zameldowania, PESEL, NIP, numer telefonu, numer IP. Poprzez RODO oraz inne przepisy prawa dotyczące ochrony danych nie wprowadza się wymogów dotyczących treści informacji, stanowiących dane osobowe. Mają one jedynie dotyczyć danej osoby, dlatego daną osobową może być IP komputera, jak również wizerunek osoby.

Zgodnie z art. 4 pkt. 2 RODO przetwarzanie oznacza „operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie". Na podstawie przytoczonej powyżej definicji nie

jest możliwe określenie, jakie czynności wchodzą w zakres pojęcia przetwarzania danych. Katalog czynności ma charakter otwarty. Gwarantuje to uniknięcie w przyszłości trudnego zadania określenia w innych przepisach prawa czynności związanych z przetwarzaniem danych.

Przetwarzanie danych osobowych, oznacza więc wszystkie działania związane z danymi osobowymi. Zarówno te mające wpływ na zmianę struktury danych, jak również takie, które takiego wpływu nie mają.

Przy analizie kwestii dotyczących danych szczególnie chronionych należy na wstępie wyartykułować jaki to rodzaj danych osobowych. Są to tzw. „dane szczególnych kategorii" (dawnej dane wrażliwe), do których zalicza się, zgodnie z art. 9 ust. 1 RODO „informacje ujawniające pochodzenie rasowe i etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne (art. 4 pkt. 13 RODO, motyw 34 RODO), biometryczne (art. 4 pkt. 14 RODO), dotyczące zdrowia (art. 4 pkt. 15 RODO, motyw 35 RODO), seksualności lub orientacji seksualnej. Ustawodawca unijny zabrania przetwarzania tego typu danych, jednakże wskazuje sytuacje, w których ADO może zgodnie z prawem operować danymi szczególnych kategorii, mając na uwadze fakt, że przesłanki legalizujące ich przetwarzanie są inne niż w przypadku danych zwykłych.

W przepisach RODO wyróżniono dane osobowe, które dotyczą wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa. W bibliotece takie dane mogą być przetwarzane m.in. w sytuacji, gdy osadzeni pod odpowiednim nadzorem wykonują prace porządkowe na rzecz biblioteki. Zgodnie z art. 10 RODO przetwarzania takich danych „wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. Wszelkie kompletne rejestry wyroków skazujących są prowadzone wyłącznie pod nadzorem władz publicznych".

Ustawodawca unijny wskazuje, że informacje dotyczące wyroków skazujących i naruszeń prawa nie stanowią szczególnej kategorii danych. Ich legalne przetwarzanie odbywa się w oparciu o art 6 ust. 1 RODO, jednakże przy jednoczesnym spełnieniu warunków z art. 10 RODO, gdzie przetwarzanie jest dopuszczone wyłącznie pod nadzorem władz publicznych lub jeżeli jest dozwolone prawem Unii lub państwa członkowskiego. Należy nadmienić, że przetwarzanie obejmuje dane dotyczące wyroków skazujących i naruszeń prawa np. z wyroków dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych. Nie obejmuje natomiast innych orzeczeń, które zostały wydane w postępowaniu sądowym i administracyjnym.

Osobną kwestię stanowi przetwarzanie danych „niewymagające identyfikacji". Zgodnie z art. 11 ust. 1 RODO, „jeżeli cele, w których administrator przetwarza dane osobowe, nie wymagają lub już nie wymagają zidentyfikowania przez niego osoby, której dane dotyczą, administrator nie ma obowiązku zachowania, uzyskania ani przetworzenia dodatkowych informacji w celu zidentyfikowania osoby, której dane dotyczą, wyłącznie po to, by zastosować się do niniejszego rozporządzenia". W ust. 2 wskazano, że „jeżeli w przypadkach, o których mowa w ust. 1 niniejszego artykułu, administrator może wykazać, że nie jest w stanie zidentyfikować osoby, której dane dotyczą, w miarę możliwości informuje o tym osobę, której dane dotyczą. W takich przypadkach zastosowania nie mają art. 15–20, chyba że osoba, której dane dotyczą, w celu wykonania praw przysługujących jej na mocy tych artykułów dostarczy dodatkowych informacji pozwalających ją zidentyfikować". W powyższym temacie jest ponadto mowa w motywie 57 RODO, który brzmi następująco: „Jeżeli dane osobowe przetwarzane przez administratora nie pozwalają mu zidentyfikować osoby fizycznej, nie powinien on mieć obowiązku uzyskania dodatkowych informacji w celu zidentyfikowania osoby, której dane dotyczą, wyłącznie po to, by zastosować się do przepisów niniejszego rozporządzenia. Administrator nie powinien jednak odmawiać przyjęcia dodatkowych informacji od osoby, której dane dotyczą, by

ułatwić jej wykonywanie jej praw. Weryfikacja tożsamości powinna obejmować cyfrową identyfikację osoby, której dane dotyczą, na przykład poprzez mechanizm uwierzytelniania, taki jak te same dane uwierzytelniające, których osoba, której dane dotyczą, używa, by zalogować się do usług internetowych oferowanych przez administratora".

Cytowane powyżej przepisy dotyczą sytuacji, kiedy ADO z uwagi na cel przetwarzania danych np. w sytuacji rozwiązania umowy lub z uwagi na sam charakter przetwarzania, nie potrzebuje identyfikacji osób, których dane przetwarza. ADO nie ma obowiązku pozyskiwania dodatkowych informacji do zidentyfikowania osoby, żeby zastosować się do RODO i wypełnić wobec niej obowiązek informacyjny, przewidziany w art. 13. Konsekwencją zapisów art. 11 jest brak możliwości korzystania przez osoby których dane dotyczą z przysługujących im praw wynikających z art. 15-20 RODO. Jednocześnie wskazano, że w sytuacji, gdy osoba, której dane dotyczą dobrowolnie dostarczy ADO dodatkowych danych pozwalających ją zidentyfikować, wówczas będzie mogła skorzystać z powyższych praw. Jednakże ADO powinien zadbać o odpowiedni przekaz informacyjny, tak aby osoba, której dane dotyczą była świadoma, że dodatkowych danych przekazywać nie musi, a jedynie może.

2.4. Zasady przetwarzania danych osobowych.

Zasady przetwarzania danych osobowych zostały wskazane w art. 5 RODO. ADO jest zobowiązany do ich przestrzegania, wdrażając odpowiednie procedury w bibliotece oraz prowadząc dokumentację potwierdzającą zgodność przetwarzania danych z obowiązującymi zasadami. Wśród podstawowych zasad ochrony danych osobowych należy wymienić:

I. Zasadę legalności, przejrzystości i rzetelności.

Każda czynność w obszarze danych osobowych musi być zgodna z przepisami prawa (określonymi albo w prawie Unii Europejskiej, albo prawie polskim). Przetwarzanie danych uważa się za zgodne z prawem w przypadkach wymienionych w art. 6 ust. 1 lub art. 9 ust. 2 RODO. Ważnym argumentem do przetwarzania danych jest dobrowolna zgoda osoby, której dane dotyczą. Przetwarzanie danych bez spełnienia co najmniej jednej z przesłanek legalizujących jest bezprawne.

Zasada przejrzystości i rzetelności została szczegółowo wyjaśniona w preambule RODO – motywy 39, 58, 60. W kontekście tej zasady ADO zobowiązany jest do udzielania osobom, których dane dotyczą, prostych, zwięzłych komunikatów dot. przetwarzania ich danych, również w formie graficznej. Zrozumiałym językiem powinny być napisane treści klauzul informacyjnych, w których osoby, których dane dotyczą winny zostać kompleksowo poinformowane o przysługujących im uprawnieniach. Kierując się wspomnianymi zasadami, ADO powinien być wiarygodny, wypełniać należycie swoje zadania w związku z przetwarzaniem danych osobowych oraz przestrzegać obowiązujących przepisów prawa w zgodzie z zasadami współżycia społecznego. Podsumowując, odpowiednie kompetencje, poczucie odpowiedzialności w związku z właściwym przetwarzaniem danych oraz sumienne wypełnianie obowiązków informacyjnych, są warunkiem niezbędnym dla osiągnięcia zgodności działań z zasadą przejrzystości i rzetelności.

II. Ograniczenie celu.

Zgodnie z tą zasadą przetwarzanie danych musi odbywać się w ściśle określonych celach. Należy zatem przyjąć, że „dane mogą być przetwarzane przez administratora tylko i wyłącznie w celu, do którego zostały zebrane. Administrator nie ma prawa wykorzystać danych osobowych (po ich zebraniu) do innych celów"[1].

III. Zasadę minimalizacji danych.

Minimalizacja danych nakłada na ADO obowiązek ograniczenia zbierania i przetwarzania danych do niezbędnego minimum, stosownie do założonego celu. Niedozwolone jest zbieranie danych „na zapas". Dane osobowe należy zbierać w konkretnych i prawnie uzasadnionych celach. Zbierać i przetwarzać można wyłącznie te dane, dzięki którym jest możliwa realizacja założonego celu.

IV. Prawidłowość.

Z tą zasadą wiąże się konieczność aktualizowania zebranych danych przez ADO w przypadku stwierdzenia, że są one nieprawdziwe lub niekompletne. Na wniosek osoby, której dane dotyczą ADO ma również obowiązek ich sprostowania. Dane osobowe powinny być aktualne, kompletne i zgodne z prawdą. Istotna rola ADO polega również na tym, że to na nim „ciąży obowiązek dbania o dane, a w razie potrzeby ich uaktualniania oraz dbania, by nie przetwarzać danych nieaktualnych i nieprawdziwych"[2]. W interesie biblioteki leży merytoryczna poprawność danych. Od ich prawidłowości zależy realizacja celu w jakim zostały zebrane i są przetwarzane.

V. Ograniczenie przechowywania.

ADO czuwa nie tylko nad prawidłowością przetwarzania danych, ale również nad właściwym ich przechowywaniem i usuwaniem. Dane osobowe powinno się przechowywać przez okres nie dłuższy niż wynika to z realizacji celu, w którym te dane zostały zebrane i są przetwarzane. Nie ma możliwości przechowywania danych bez ograniczenia czasowego. W przepisach obowiązującego prawa (np. prawo pracy, prawo podatkowe, ustawa o rachunkowości), prawnym interesie ADO (np. okres roszczeń cywilno-prawnych), jak również w wewnętrznych regulacjach w bibliotece (np. instrukcji kancelaryjnej) doprecyzowuje się kwestię dotyczącą czasu przetwarzania danych osobowych. Określa się okres ich przechowywania, a w przypadku instrukcji kancelaryjnej dodatkowo sposób ich niszczenia. Jeżeli dane przetwarzane są na podstawie zgody osoby, której dane dotyczą to w takiej sytuacji przetwarzanie odbywa się do momentu wycofania zgody, jednak nie dłużej niż wymaga tego realizacja celu. Istotne znaczenie ma więc ustalenie terminu usuwania danych lub co najmniej okresowego ich przeglądu.

VI. Zasada rozliczalności.

W myśl tej zasady ADO odpowiada za respektowanie powyższych zasad wynikających z art. 5 RODO i musi wykazać, że ich przestrzega na każdym etapie przetwarzania danych. ADO może uar-

[1] T. Banyś, P. Biały, T. Błoński, P. Glen, M. Kwiatkowska-Cylke, J. Łuczak, Ł. Onysyk, A. Kręcisz-Sarna, M. Sarna, J. Sobczak, A. Stępień, *RODO Przewodnik po kluczowych zmianach*, Wyd. Wiedza i Praktyka, Warszawa 2018, s. 14.

[2] Tamże, s. 15.

gumentować poprawność swoich działań w przedmiotowym temacie np. poprzez prowadzenie rejestru czynności przetwarzania, opracowanie wewnętrznych procedur dotyczących ochrony danych osobowych, nadanie osobom odpowiedzialnym za przetwarzanie danych w bibliotece stosownych upoważnień i odnotowywanie tego faktu w rejestrze upoważnień. Kwestia dotycząca dokumentacji przetwarzania danych osobowych z jednoczesnym uwzględnieniem zasady rozliczalności została opisana w wytycznych na stronie Urzędu Ochrony Danych Osobowych. Wskazano tam, że „obecnie, w nowym systemie prawnym dotyczącym przetwarzania danych osobowych, nie wymienia się dokumentów jakie administrator powinien posiadać, aby wykazać zgodność realizowanych czynności przetwarzania(...). Z treści art. 24 ust 1 RODO wynika jednak, że administrator danych ma być w stanie wykazać całościowo zgodność przetwarzania danych. W praktyce oznacza to, że administrator ma obowiązek wykazać, że: stosuje się do ogólnych zasad przetwarzania określonych w art. 5 RODO"[3]. Według wytycznych Urzędu, obowiązująca w instytucji polityka bezpieczeństwa i instrukcja zarządzania systemami informatycznymi, dotyczące przetwarzania danych osobowych, mogą stanowić filar dokumentacji, której celem będzie wykazanie zgodności przetwarzania danych z wymaganiami RODO.

Na stronie internetowej UODO wskazano także, że „nową, zgodną z RODO dokumentację przetwarzania danych osobowych, która będzie jednocześnie instrumentem wykazującym zgodność wykonywanych czynności przetwarzania z przepisami prawa, występujące w dotychczasowej dokumentacji elementy należy uzupełnić dodatkowo o takie elementy jak:

- rejestr czynności przetwarzania i zakres rejestru kategorii czynności przetwarzania, o których mowa w art. 30 RODO,
- wytyczne dotyczące klasyfikacji naruszeń i procedurę zgłaszanie naruszenie ochrony danych do organu nadzorczego (UODO) – art. 33 ust. 3 RODO,
- procedurę na wypadek wystąpienia naruszeń mogących powodować wysokie ryzyko naruszenia praw i wolności osób, w zakresie ich informowaniu o działaniach jakie powinni wykonać, aby ryzyko to ograniczyć – art. 34 RODO,
- procedurę prowadzenia wewnętrznej dokumentacji stanowiącej rejestr naruszeń ochrony danych, o którym mowa w art. 33 ust 5 RODO,
- raport z przeprowadzonej, ogólnej analizy ryzyka,
- raport z ocen skutków dla ochrony danych – art. 35 ust. 7. – jeśli dotyczy,
- procedury związane z pseudonimizacją i szyfrowaniem – jeśli dotyczy,
- plan ciągłości działania – art. 32 ust 1 pkt b RODO,
- procedury odtwarzania systemu po awarii, oraz ich testowania – art. 32 ust 1 pkt c i d RODO[4].

Przygotowanie w/w dokumentacji i stosowanie się do jej wytycznych pozwala ADO rozliczyć się ze stosowania zasad dotyczących ochrony danych na każdym etapie ich przetwarzania.

Warto także zwrócić uwagę na integralność i poufność. Do tej zasady odnosi się art. 32 RODO. ADO na podstawie przeprowadzonej analizy ryzyka ma obowiązek wprowadzić w bibliotece szerokie spektrum środków organizacyjnych i technicznych celem zabezpieczenia danych osobowych. Nienaruszalność zgromadzonych danych oraz zapewnienie, że dane nie zostaną udostępnione lub ujawnione osobom nieupoważnionym stawia przed ADO konieczność zastosowania odpowiednich narzędzi technicznych w bibliotece, żeby wykluczyć ryzyko nielegalnego ich przetwarzania, uchronić dane przed ewentualną utratą czy uszkodzeniem. W obowiązującej w bibliotece dokumentacji dotyczącej ochrony danych osobowych należy wskazać pracownikom jak właściwie zabezpieczać dane

[3] *Strona internetowa Urzędu Ochrony Danych Osobowych*, www.uodo.gov.pl/pl/138/273 [dostęp 30.09.2019 r.].
[4] Tamże.

osobowe, np. poprzez zabezpieczenie komputera hasłem, nie udostępnianie haseł innym osobom, nie zapisywanie haseł na kartce, nie otwieranie załączników z wiadomości e-mail niewiadomego pochodzenia oraz nie otwieranie linków w podejrzanych wiadomościach, stosowanie programów antywirusowych, zamykanie dokumentacji papierowej w szafkach, odpowiednio zabezpieczając klucze, niszczenie dokumentów za pomocą niszczarek, itp. Precyzyjnie określone zasady postępowania i należyte ich stosowanie minimalizują ryzyko zawiązane z naruszeniem danych i konsekwencjami z tym związanymi.

2.5. Przesłanki legalności przetwarzania zwykłych i szczególnych kategorii danych.

Zgodnie z RODO, w przypadku danych zwykłych, administrator ma prawo przetwarzać dane realizując swoje zadania na podstawie sześciu przesłanek. Każda z nich jest obarczona innymi obowiązkami. Wszystkie z przesłanek zawarte są w art. 6 RODO. Są to: zgoda osoby, której dane dotyczą; wykonanie umowy, której stroną jest osoba, której dane dotyczą; realizacja obowiązku prawnego ciążącego na administratorze; ochrona żywotnych interesów osób, wykonanie przez administratora zadania w interesie publicznym lub w ramach sprawowania władzy publicznej; oraz przetwarzanie przez administratora danych wymaga zrealizowania jego prawnie uzasadnionego interesu.

Przetwarzanie danych na podstawie zgody powinno być dokonywane tylko w przypadku, gdy nie zachodzi żadna inna przesłanka do przetwarzania. Daje także osobom, których dane są przetwarzane na podstawie zgody największą liczbę praw przysługujących na mocy przepisów RODO. Zgoda musi być dobrowolna i nie można od niej uzależniać realizacji innych celów opartych na pozostałych przesłankach, np. nie można żądać zgody na wysyłanie newslettera w połączeniu z możliwością zapisania się do biblioteki. Należy pamiętać, że osoba, której dane dotyczą ma możliwość wycofania danej zgody w dowolnym momencie, co sprawia, że opieranie działalności kluczowych obszarów funkcjonowania jednostki na tej właśnie przesłance może doprowadzić do paraliżu tejże działalności. Nie należy nadużywać formy zgody. Nie należy w żadnym wypadku pobierać zgody, jeśli przetwarzanie będzie się odbywać na innej podstawie prawnej. Na przykład nie należy używać zgody, gdy czytelnik zapisuje się do biblioteki. W takim przypadku czytelnik jest zobowiązany do podania danych na podstawie przepisu prawa i nie należy w żadnym formularzu wpisywać, że osoba zapisując się do biblioteki „wyraża zgodę", gdyż przetwarzanie danych nie będzie się na tej „zgodzie" opierało. W bibliotece przetwarzanie na podstawie zgody może odbywać się w celu przetwarzania danych kontaktowych czytelnika (np. nr telefonu, adres e-mail), wysyłania newsletteru, czy rozpowszechniania wizerunku.

Kolejną przesłanką legalizującą przetwarzanie jest wykonanie umowy. Korzystanie z tej przesłanki będzie zachodziło zawsze, gdy administrator i osoba, której dane dotyczą będą stronami umowy. Podanie danych do przygotowania i realizacji umowy jest obowiązkowe, jeśli osoba, której dane dotyczą chce, by taka umowa była zawarta. Biblioteka może przetwarzać dane na podstawie tej przesłanki wówczas, gdy zawiera z osobą fizyczną umowę na prowadzenie zajęć w jednostce.

Wypełnienie obowiązku prawnego ciążącego na administratorze także zobowiązuje osobę, której dane dotyczą, do podania danych w każdym przypadku, gdy taka osoba chce skorzystać z określonych uprawnień przewidzianych w prawie. Przykładem takich okoliczności jest zatrudnienie na podstawie Kodeksu pracy, kiedy osoba, której dane dotyczą, musi podać określony, wskazany w przepisach zakres danych, by mogła zostać zawarta umowę o pracę.

Kolejną przesłanką legalizującą przetwarzanie, jest konieczność wypełnienia obowiązku prawnego ciążącego na administratorze, gdy przetwarzanie jakiego dokonuje jest w interesie publicznym lub w związku ze sprawowaniem władzy publicznej. W obydwu powyższych przesłankach administrator powinien swoje działania opierać na prawie unijnym lub prawie państwowym, gdzie będzie jasno określony cel przetwarzania.

Możliwość przetwarzania danych dla ochrony prawnie uzasadnionych interesów osób fizycznych zachodzi tylko wówczas, gdy nie ma możliwości oparcia przetwarzania o inną podstawę prawną, a decyzja o braku przetwarzania będzie grozić negatywnymi skutkami dla tych osób. Przykładem mogą być ostrzeżenia o warunkach pogodowych wysyłane za pomocą sieci komórkowych.

Ostatnią z przesłanek legalizujących przetwarzanie jest prawnie uzasadniony interes administratora. Przetwarzanie na podstawie tej przesłanki może zdarzać się wówczas, gdy osoba, której dane dotyczą, może oczekiwać, że do takiego przetwarzania może dojść. Ma to miejsce w przypadku windykacji należności od czytelnika za nieterminowy zwrot materiałów bibliotecznych lub w przypadku prowadzenia monitoringu dla zapewnienia bezpieczeństwa osób lub mienia. Przy korzystaniu z tej przesłanki, należy dokonać testu wagi prawnie uzasadnionych interesów biblioteki oraz osób, których dane dotyczą, ponieważ jej stosowanie jest niedopuszczalne, jeżeli interes osoby, której dane dotyczą, będzie stał wyżej aniżeli prawnie uzasadniony interes biblioteki. Przesłanka ta nie powinna być także wykorzystywana przez organy publiczne wykonujące swoje zadania, gdyż sposób wykonania takich zadań powinien być określony w przepisach powszechnie obowiązującego prawa.

Odrębnym zasadom podlega przetwarzanie omówionych w podrozdziale 2.3. danych szczególnych kategorii, do których w RODO zaliczono dane ujawniające pochodzenie etniczne lub rasowe, poglądy polityczne, wyznanie, przekonania światopoglądowe, przynależność do związków zawodowych, danych genetycznych, dotyczących zdrowia, orientacji seksualnej i seksualności. Przetwarzanie takich danych, zgodnie z art. 9 ust. 2 RODO jest możliwe tylko wtedy, gdy:

- osoba, której dane dotyczą wyrazi na takie przetwarzanie zgodę,
- przetwarzanie jest niezbędne do zrealizowania obowiązków lub uprawnień wynikających z przepisów prawa,
- osoba, której dane dotyczą nie może wyrazić zgody, ale przetwarzanie jest niezbędne do ochrony jej żywotnych interesów,
- przetwarzania dokonuje podmiot w ramach swojej działalności a przetwarzanie dotyczy wyłącznie członków, byłych członków lub osób utrzymujących kontakty z tym podmiotem w związku z celami jego działalności a dane nie są ujawniane poza ten podmiot bez zgody osób, których dane dotyczą,
- przetwarzanie dotyczy publicznie udostępnionych danych przez osobę, której dane dotyczą,
- przetwarzanie jest niezbędne do ochrony roszczeń lub jest związane ze sprawowaniem wymiaru sprawiedliwości przez sądy,
- przetwarzanie jest związane z ważnym interesem publicznym, ma swoje oparcie w przepisach prawa i nie narusza istoty prawa do ochrony praw podstawowych i interesów osoby, której dane dotyczą,
- jest niezbędne do celów związanych z profilaktyką zdrowotną lub medycyną pracy, także w przypadku oceny zdolności do pracy;
- jest niezbędne dla zapewnienia ochrony przed zagrożeniami zdrowotnymi,
- jest niezbędne do celów archiwalnych, badań naukowych, historycznych lub statystycznych, ma swoje oparcie w przepisach prawa i nie narusza istoty prawa do ochrony praw podstawowych i interesów osoby, której dane dotyczą.

Poza wymienionymi przesłankami przetwarzanie danych szczególnych kategorii jest zabronione.

Poprzez przepisy RODO dano możliwość doprecyzowania państwom Unii Europejskiej w zakresie możliwości przetwarzania danych genetycznych, biometrycznych i dotyczących zdrowia. Na tej podstawie w polskim prawie pracy znalazły się zapisy o możliwości wykorzystania danych biometrycznych do zabezpieczenia szczególnie ważnych informacji lub zabezpieczenia dostępu do pomieszczeń wymagających szczególnej ochrony. W przypadku bibliotek mogą to być pomieszczenia, w których przechowuje się szczególnie ważne i cenne dla kultury polskiej zabytki piśmiennictwa lub informacje niejawne.

Ponadto biblioteki mogą przetwarzać dane szczególnych kategorii, w związku z realizowaniem obowiązków wynikających z przepisów prawa pracy. Przetwarzane mogą wtedy być informacje o ocenie stanu zdrowia pracowników, tzn. ich zdolności do pracy na określonym stanowisku, a także dane związane z korzystaniem ze zwolnień lekarskich lub szczególnych uprawnień, np. w związku ze stwierdzoną niepełnosprawności. Biblioteka, jako pracodawca, może także przetwarzać dane pracowników w zakresie przynależności do organizacji związkowej, gdy pracownikowi należą się specjalne uprawnienia związane z jego działalnością związkową.

2.6. Problematyka przetwarzania danych osobowych dzieci.

Omawiając problematykę legalności przetwarzania danych osobowych dzieci, należy w pierwszej kolejności odwołać się do przepisów kodeksu cywilnego. Zgodnie z art. 12 KC „nie mają zdolności do czynności prawnych osoby, które nie ukończyły lat trzynastu". Po ukończeniu 13 roku życia dziecko nabywa częściową zdolność do podejmowania czynności prawnych, ale jedynie w zakresie drobnych spraw życia codziennego. W pozostałych przypadkach, aby czynność prawna wykonana przez małoletniego była ważna, musi zostać potwierdzona przez rodzica lub opiekuna prawnego (art. 15 i 20 KC). Pojęcie „drobnych bieżących spraw życia codziennego" nie zostało w przepisach zdefiniowane, jednak można uznać, że oznacza ono sprawy, które z obiektywnego punktu widzenia są niewielkiej wagi, jak drobne zakupy, czy udział w szkolnym konkursie, gdzie nagroda jest niewielkiej wartości. Odnosząc się do zagadnienia legalności przetwarzania danych osobowych dzieci, to mają zastosowanie te same przesłanki legalizujące przetwarzanie, jak do danych osób dorosłych, w szczególności przetwarzanie danych dzieci jest dozwolone jeżeli wynika z przepisów powszechnie obowiązującego prawa (jak prawo oświatowe), czy jest realizowane w interesie publicznym. W pewnych okolicznościach będzie można także powołać się na przesłankę prawnie uzasadnionego interesu administratora, np. w związku z wyróżnianiem najlepszych czytelników, ponieważ takie działanie wpisuje się w statutowe cele biblioteki, jakimi jest promocja czytelnictwa i nie występują nadrzędne interesy osób, których dane dotyczą.

Przepisy Kodeksu cywilnego ograniczają możliwość zawarcia przez małoletniego umowy, której byłby stroną. Taka umowa będzie ważna, tylko pod warunkiem zakwalifikowania jako drobna sprawa życia codziennego. W związku z tym rozważając możliwość samodzielnego zapisania się przez dziecko do biblioteki, należy stwierdzić, że jeżeli nie ukończyło ono 13 roku życia, to nie może ono dokonać tej czynności samodzielnie, gdyż dziecko nie jest w stanie skutecznie zaakceptować regulaminu biblioteki. W takim wypadku niezbędne jest pośredniczenie opiekuna ustawowego, tzn. rodzica lub opiekuna prawnego, w czynności zapisu do biblioteki. Rozważając możliwość zapisania małoletniego, który ukończył 13 rok życia, należy wziąć pod uwagę ewentualne negatywne skutki związane z zapisem, w szczególności wysokość ewentualnej kary za nieterminowy zwrot materiałów bibliotecznych. Jeżeli kwota kary byłaby drobna, można uznać, że jest to czynność z kategorii drobnych spraw, jeżeli może być znaczna, małoletni nie powinien samodzielnie dokonywać takiej czynności praw-

nej. Podobnie należy rozważyć możliwość przetwarzania danych małoletnich powyżej 13 roku życia w kontekście korzystania z udostępnień na miejscu, czy pracowni internetowej.

Odrębnego omówienia wymaga możliwość wyrażenia zgody na przetwarzanie danych osobowych. W pierwszej kolejności należy uwzględnić przepisy szczególne, czyli ponownie jeżeli sprawa będzie z kategorii drobnych spraw życia codziennego, to małoletni, który ukończył 13 rok życia, będzie mógł skutecznie wyrazić zgodę. Takim działaniem może być udział w konkursie lub korzystanie z bezpłatnych zajęć bibliotecznych. Jednakże przepisy RODO przewidują wyjątek od tej reguły. Zgodnie z art. 8 korzystanie z usług społeczeństwa informacyjnego, czyli świadczonych świadczoną za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług. W takim przypadku osoba małoletnia, może wyrazić zgodę, by skorzystać z takich usług dopiero po ukończeniu 16 roku życia,. Co prawda unijny ustawodawca dał możliwość krajom unijnym obniżenia granicy wieku do lat 13, jednak polski ustawodawca nie skorzystał z tej możliwości. W przeciwnym wypadku niezbędna jest zgoda opiekuna ustawowego. Należy jednak zauważyć, że co do zasady biblioteki nie świadczą usług określanych jako usługi społeczeństwa informacyjnego. Chociażby OPAC nie spełnia tych kryteriów, gdyż jest usługą nieodpłatną. Przykładem usługi społeczeństwa informacyjnego mogłoby być płatne szkolenie online.

Jeżeli korzystanie z innych działalności prowadzonych w bibliotekach przez dzieci wymaga zgody, powinno się odbywać za pośrednictwem ich rodziców lub opiekunów prawnych. Chodzi tutaj zarówno o usługi powiązane bezpośrednio z działalnością biblioteczną placówki, jak i związane z szeroko pojętą kulturą, które biblioteka może udostępniać w związku z tym, że jest instytucją kultury. Do tych pierwszych należy przede wszystkim zaliczyć dostęp do informacji za pośrednictwem sieci Internet. Bardzo dobrym wyjściem jest powiązanie możliwości korzystania ze wszystkich zasobów biblioteki z kartą biblioteczną. Natomiast jeśli chodzi o usługi kulturalne należy przede wszystkim wymienić wszelkie zajęcia, warsztaty, konkursy, do których niezbędne jest zapisanie uczestników. W każdym z takich przypadków, gdy wymagane jest przetwarzanie danych osób małoletnich, pośrednikiem pomiędzy biblioteką a dzieckiem powinien być rodzic lub opiekun prawny, chyba że małoletni ukończył 13 lat, działanie podlega pod kategorię drobnych spraw życia codziennego i nie jest usługą społeczeństwa informacyjnego.

Na nieco innych zasadach działają biblioteki szkolne. Podstawą prawną dla działania tych bibliotek są zarówno ustawa o bibliotekach, jak i Prawo oświatowe. Przepisy odgórne określają, że szkolne placówki biblioteczne, z racji bycia częścią placówek oświatowych, stanowią przede wszystkim wsparcie dla realizacji zadań edukacyjnych. Tym samym nie są one administratorami danych osobowych, gdyż nie decydują samodzielne w swojej działalności o celach i środkach przetwarzania danych. W związku z powyższym dane osobowe w bibliotekach szkolnych przetwarzane są w związku z edukacyjną działalnością szkoły a małoletnimi użytkownikami tych bibliotek są uczniowie konkretnej placówki oświatowej. Szkoła jest zatem administratorem danych przetwarzanych w bibliotece, i to na niej spoczywają wszelkie prawa i obowiązki związane z systemem ochrony danych osobowych.

2.7. Dobre praktyki, wytyczne i wskazówki.

Zgoda na przetwarzanie danych

Elementy zgody

Zgoda powinna być wyrażana w konkretnym celu lub tożsamych celach. Nie powinna być to ogólna zgoda „na przetwarzanie danych". Na przykład można wyrazić zgodę na upublicznienie zdjęcia na stronie w celu promocji wydarzenia, którego było się uczestnikiem. Zgoda powinna być wyrażana dla konkretnego administratora. Osoba, której dane dotyczą powinna wiedzieć, że może ją wycofać w dowolnym momencie i że jest dobrowolna. Zatem minimalne elementy zgody to:

- dane administratora,
- cel przetwarzania,
- informacja o możliwości wycofania zgody wraz z jej konsekwencjami,
- informacja o dobrowolności wyrażenia zgody.

Ogólna klauzula zgody wersja

Wyrażam zgodę na przetwarzanie moich danych przez **[dane administratora, tzn. pełna nazwa, dane kontaktowe]** w celu **[wskazać konkretny cel, np. otrzymywanie newslettera]**. Zostałem/am poinformowany/a, że zgodę mogę wycofać w dowolnym momencie i jest ona dobrowolna.

Ogólna klauzula zgody wersja – dziecko

Zgadzam się na przetwarzanie danych mojego dziecka **[imię i nazwisko dziecka]** przez **[dane administratora, tzn. pełna nazwa, dane kontaktowe]** w celu **[wskazać konkretny cel, np. otrzymywanie newslettera]**. Zostałem/am poinformowany/a, że zgodę mogę wycofać w dowolnym momencie i jest ona dobrowolna.

3 DANE OSOBOWE PRACOWNIKÓW BIBLIOTEKI I PRZETWARZANIE DANYCH OSOBOWYCH PRZEZ PRACOWNIKÓW BIBLIOTEKI

3.1. Prawne podstawy przetwarzania danych osobowych pracowników.

I. Dane niezbędne do zawarcia stosunku pracy.

Prawne podstawy przetwarzania danych osobowych pracowników zostały wyartykułowane w Kodeksie pracy. Na podstawie art. 22^1 § 1 KP pracodawca ma prawo żądać od osoby ubiegającej się o zatrudnienie podania danych osobowych obejmujących:

- imię (imiona) i nazwisko,
- datę urodzenia,
- dane kontaktowe wskazane przez taką osobę,
- wykształcenie,
- kwalifikacje zawodowe,
- przebieg dotychczasowego zatrudnienia.

Warto zwrócić uwagę, że ustawodawca precyzyjnie wskazuje, że pracownik podaje informacje o wykształceniu, kwalifikacjach zawodowych i przebiegu dotychczasowego zatrudnienia, gdy jest to niezbędne do wykonywania pracy określonego rodzaju lub na określonym stanowisku.

Zgodnie z art 22^1 § 3 KP pracodawca żąda od pracownika podania dodatkowych danych osobowych, które obejmują:

- adres zamieszkania,
- numer PESEL (a w przypadku jego braku rodzaj i numer dokumentu potwierdzającego tożsamość),
- inne dane osobowe pracownika, a także dane osobowe dzieci pracownika i innych członków jego najbliższej rodziny, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy,
- wykształcenie i przebieg dotychczasowego zatrudnienia (jeżeli nie istniała podstawa do ich żądania od osoby ubiegającej się o zatrudnienie),
- numer rachunku płatniczego (jeżeli pracownik nie złożył wniosku o wypłatę wynagrodzenia do rąk własnych).

Zgodnie z art 22^1 § 4 KP pracodawca żąda podania także innych danych osobowych, gdy jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Udostępnienie pracodawcy danych osobowych następuje w formie oświadczenia osoby, któ-

rej dane dotyczą. Pracodawca ma prawo żądać od pracownika, innych jego danych osobowych, a także imion i nazwisk oraz dat urodzenia jego dzieci, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez niego ze szczególnych uprawnień przewidzianych w prawie pracy, np. z uwagi na przysługujące pracownikowi dwa dni w roku opieki w nad dzieckiem do 14 roku życia na podstawie art. 188 kodeksu pracy oraz w związku ze sprawowaniem opieki nad chorym dzieckiem, gdzie koniecznym jest wypełnienie wniosku o zasiłek opiekuńczy Z-15A, w oparciu o ustawę z dnia 25 czerwca 1999 r. o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa.

Dane osobowe niezbędne do zawarcia stosunku pracy pracodawca przetwarza zgodnie z przepisami Kodeksu pracy, spełniona jest więc przesłanka legalności z art. 6 ust. 1 lit. c RODO. Zgodnie z tym przepisem przetwarzanie jest dopuszczalne, gdy jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze. Przetwarzanie innych danych osobowych niż te wymienione powyżej jest dopuszczalne tylko za zgodą osoby zatrudnionej.

Pracodawca będzie także przetwarzał dane szczególnych kategorii, o których mowa w art. 9 ust. 1 RODO, w zakresie danych o stanie zdrowia pracownika, jak informacje związane ze zwolnieniami lekarskimi, czy orzeczeniami lekarskimi o zdolności do pracy, w których lekarz medycyny pracy wskazał dodatkowe informacje dotyczące stanu zdrowia, np. konieczność pracy w okularach. Przetwarzanie tych danych jest obowiązkiem pracodawcy i odbywa się w zgodzie z przesłanką legalizującą z art. 9 ust. 2 lit. b RODO.

Dobrowolna zgoda pracownika jest niezbędna: na przetwarzanie wizerunku pracownika (np. w celu publikacji jego zdjęcia w Internecie), danych o jego zainteresowaniach (np. gdy będą planowane firmowe wycieczki), danych współmałżonka (np. w sytuacji, gdy będą przesyłane świąteczne prezenty do jego żony lub męża). Udzielenia dobrowolnej zgody wymaga również umieszczenie zdjęcia na identyfikatorze pracownika. Jedynie w niektórych sytuacjach, gdy wizerunek pracownika jest ściśle związany z wykonywanym przez niego zawodem lub charakterem pracy i wskazywanie wizerunku pracownika przewidują przepisy prawa, zgoda nie jest wymagana.

Zgodnie z art. 13 ust. 1 i ust. 2 RODO biblioteka, jako administrator danych ma obowiązek przygotować klauzulę informacyjną dla pracownika, z którą musi zapoznać się każdy nowo zatrudniony. Treść klauzuli powinna być dostępna dla wszystkich zatrudnionych w instytucji pracowników np. w dziale organizacyjnym biblioteki.

II. Dane niezbędne do realizacji stażów i praktyk bibliotecznych.

W przypadku przetwarzania danych osobowych stażystów i praktykantów mają zastosowanie odpowiednio przepisy:

- dla praktyk uczniowskich – Prawo oświatowe,
- dla praktyk studenckich – Prawo o szkolnictwie wyższym i nauce oraz ustawy o praktykach absolwenckich,
- dla stażystów z urzędu pracy - ustawy o promocji zatrudnienia i instytucjach rynku pracy.

Celem przetwarzania danych osobowych jest zawarcie i realizacja umowy lub porozumienia zawartych z innym podmiotem (urząd pracy, szkoła wyższa) dotyczących odbywania stażu lub praktyki w bibliotece, a także wypełnienie obowiązków prawnych biblioteki związanych z realizacją stażu lub praktyki wynikające z przepisów prawa. Biblioteka, jako ADO pozyskuje także niezbędne dane wynikające z przepisów podatkowych oraz o ubezpieczeniu społecznym. Podstawa do przetwarzania tych danych jest wskazana w przepisach powszechnie obowiązującego prawa, więc spełniony jest warunek legalności z artykułu 6 ust. 1 lit. c RODO. Przetwarzanie danych tych osób może odbywać

się również na podstawie udzielonej zgody, np. do celów kontaktowych (prywatny nr telefonu, prywatny adres e-mail) lub na publikację wizerunku na stronie internetowej.

W rozporządzeniu MEN w sprawie praktycznej nauki zawodu w § 7 ust. 3 określono, że szkoła i podmiot, w którym będą odbywały się praktyki lub staż zawierają umowę, która zawiera dane osobowe stażysty lub praktykanta. Oznacza to, że pomiędzy szkołą i biblioteką dochodzi do udostępnienia danych osobowych, w związku z realizowaniem obowiązku wynikającego z przepisów prawa. Zgodnie z art. 14 ust. 5 lit. c RODO obowiązku informacyjnego administrator nie musi realizować, gdy przekazanie danych wynika bezpośrednio z przepisu prawa. Wobec powyższego nie ma konieczności spełnienia obowiązku informacyjnego wobec tych osób.

III. Dane osobowe zleceniobiorców.

Podstawą przetwarzania danych osobowych zleceniobiorców, z którymi zawierane są umowy cywilnoprawne, jest konieczność wykonania postanowień umowy oraz niezbędność do podjęcia działań na żądanie osoby, której dane dotyczą przed zawarciem umowy (art. 6 ust. 1 lit. b RODO). Poza danymi niezbędnymi do zawarcia umowy (tzn. dane identyfikacyjne), ADO przetwarza także inne dane, ze względu na ciążące na nim obowiązki prawne, np. w związku ze zgłoszeniem do ubezpieczenia zdrowotnego (art. 6 ust. 1 lit. c RODO). Wobec osób zatrudnionych w ramach umów cywilnoprawnych nie mają zastosowania przepisy Kodeksu pracy, gdyż takie umowy są kształtowane na podstawie przepisów Kodeksu cywilnego. W prawie cywilnym akceptowana jest zasada swobody umów, która umożliwia dowolne kształtowanie treści umów, o ile nie sprzeciwia się to charakterowi i naturze stosunku zobowiązaniowego. Przy zbieraniu danych należy dokonać analizy adekwatności ich zakresu do celu, tzn. zbieranie których informacji jest konieczne w związku z realizacją umowy i obowiązkami wynikającymi z umowy (np. wypłata wynagrodzenia) lub z przepisów prawa (np. konieczność opłaty składek na ubezpieczenie zdrowotne lub społeczne, odprowadzenie podatku dochodowego). Jeżeli przy zatrudnieniu osób na umowy cywilnoprawne nie mają zastosowania przepisy Kodeksu pracy, należy mieć na uwadze ograniczony zakres danych osobowych, które mogą być w tej sytuacji przetwarzane przez bibliotekę w związku z realizacją postanowień umowy i wypełnieniem obowiązku prawnego przez zleceniodawcę (ADO). Należy podkreślić, że przetwarzanie danych zleceniobiorców odbywa się również na podstawie wyrażonej przez nich dobrowolnej zgody np. w celach ułatwiających zleceniodawcy kontakt np. poprzez podanie prywatnego nr telefonu, prywatnego adresu e mail, lub zgody na publikację wizerunku na stronie internetowej, w mediach społecznościowych itp.

IV. Wizerunek pracownika na stronie internetowej oraz w mediach społecznościowych.

Wizerunek zaliczany jest do danych osobowych, dlatego też powinien być w odpowiedni sposób chroniony, w oparciu o przepisy Prawa autorskiego a także przepisów o ochronie danych osobowych. W przepisach KC rozszerzono definicję o określenie wizerunku człowieka jako jego dobra osobistego, podlegającego szczególnej ochronie. Wskazanie wizerunku jako dobra osobistego znajduje się w art. 23 Kodeksu cywilnego w brzmieniu: „Dobra osobiste człowieka, jak w szczególności zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska, pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych prze-

pisach". Rozpowszechnianie przez pracodawcę wizerunku pracownika, stażysty, praktykanta, czy zleceniobiorcy musi odbywać się na podstawie zgody tej osoby, w której powinien zostać wskazany cel rozpowszechniania wizerunku, np. promocyjny, informacyjny. Pracodawca, który upublicznia wizerunek pracownika, przetwarza jego dane osobowe. Oprócz uzyskania zgody powinien wypełnić obowiązek informacyjny. Przepisy Prawa autorskiego określają sytuacje, w której wyrażenie zgody na publikację wizerunku nie jest wymagane. Nie wymaga się zgody od osoby powszechnie znanej, gdy konieczność wykorzystania wizerunku tej osoby wynika z przepisów prawa; kiedy osoba, której wizerunek będzie wykorzystywany stanowi szczegół całości (np. zgromadzenia, krajobrazu lub publicznej imprezy) lub gdy osoba otrzymała zapłatę za pozowanie. Dla celów dowodowych ADO powinien uzyskać zgodę osoby, której dane dotyczą na piśmie. Zgoda na publikację wizerunku powinna zawierać: datę i miejsce jej udzielenia, cel wykorzystania wizerunku (promocyjny, reklamowy, informacyjny), czas, na jaki została udzielona, imię, nazwisko oraz podpis pracownika. Należy także pamiętać o wymaganiach wynikających z Prawa autorskiego, w szczególności o wskazaniu, że jest to zgoda na nieodpłatne rozpowszechnienie (gdyż co do zasady za takie działanie należy się wynagrodzenie), a także jakie będą pola eksploatacji (miejsca i forma publikacji zdjęcia, np. strona internetowa biblioteki). Reasumując, publikacja wizerunku na stronie internetowej, czy w mediach społecznościowych wymaga uzyskania jego dobrowolnej zgody.

W niektórych sytuacjach umieszczanie zdjęć pracownika lub współpracownika w Intranecie, tzn. w ramach wewnętrznego systemu pracodawcy, do którego dostęp ma ściśle określony krąg osób, jak pracownicy, którzy znają się nawzajem, oraz z uwagi na cel, jaki przyświeca tego typu działaniom pracodawcy, jakim jest usprawnienie procesu zarządzania i wewnętrznej komunikacji w firmie, jest dopuszczalne bez uzyskania odrębnej zgody, w oparciu o prawnie usprawiedliwiony interes administratora (art. 6 ust. 1 lit. f RODO). Umożliwia to bowiem identyfikację pracownika w ramach wykonywanych przez niego obowiązków. W takim przypadku umieszczenie zdjęć w Intranecie służy, np. polepszeniu i usprawnieniu zarządzania biblioteką.

V. Przetwarzanie danych w związku z monitoringiem wizyjnym.

Biblioteka, jako ADO ma obowiązek chronić wizerunki pracowników oraz innych osób, odwiedzających bibliotekę, utrwalone za pośrednictwem monitoringu wizyjnego. Pracodawca może wprowadzić ten szczególny środek nadzoru na terenie biblioteki w oparciu o przepisy Kodeksu pracy. Celem precyzyjnego określenia zasad przetwarzania danych osobowych z użyciem monitoringu wizyjnego należy dokonać oceny skutków dla ochrony danych, która służy wykazaniu niezbędności wprowadzenia monitoringu. Niezbędność, jest warunkiem wynikającym z przepisów KP, czyli pracodawca nie ma pełnej dowolności w decydowaniu o wprowadzeniu monitoringu. Następnie pracodawca jest zobligowany powiadomić pracowników w formie przyjętej u pracodawcy (regulamin pracy, obwieszczenie) oraz oznaczyć teren monitorowany i udostępnić klauzulę informacyjną. Praktykuje się wprowadzenie do Regulaminu Pracy obowiązującego w jednostce odpowiednich zapisów informujących między innymi, że w celu ochrony bezpieczeństwa pracowników zatrudnionych w bibliotece oraz zabezpieczenia mienia należącego do Pracodawcy, a także zapobieżenia czynom skierowanym przeciwko zatrudnionym lub mieniu Pracodawcy, wprowadzony został monitoring wizyjny, polegający na rejestrowaniu obrazu przez zamontowane kamery, w siedzibie biblioteki. Zalecane jest także określenie w regulaminie lub odrębnej procedurze kto ma dostęp do zarejestrowanego obrazu, kto pełni nadzór nad urządzeniami oraz jaki jest okres przechowywania nagrań.

VI. Obowiązki informacyjne wobec pracownika.

Zgodnie z art. 13 ust.1 i ust. 2 RODO administrator danych ma obowiązek przygotować klauzulę informacyjną dla pracownika, którą musi udostępnić wszystkim pracownikom. Treść klauzuli powinna być dostępna w dziale kadr biblioteki oraz u IOD. Klauzulę informacyjną placówka może udostępnić również pracownikom w formie elektronicznej np. za pośrednictwem elektronicznego systemu wymiany dokumentów, w Intranecie, w kwestionariuszu osobowym lub na stronie internetowej biblioteki. Klauzula nie wymaga podpisu ani zgody, jednakże wielu pracodawców prosi pracowników o oświadczenie o zapoznaniu się wraz z datą i podpisem, aby dołączyć ją do akt pracownika. Obowiązek informacyjny wypełnia się także wobec stażystów, praktykantów oraz zleceniobiorców. W przypadku zleceniobiorców, może stanowić część treści umowy cywilnoprawnej.

VII. Dane służbowe pracownika.

Dane pracowników biblioteki takie jak np. imię i nazwisko, stanowisko, służbowy numer telefonu, czy służbowy adres e-mail, umieszczane w dokumentach, np. umowach, formularzach, czy na stronie internetowej instytucji, nazywane są „danymi służbowymi", gdyż ściśle wiążą się z wykonywaniem przez pracowników obowiązków służbowych. Dane te mogą być wykorzystywane (np. udostępniane) przez pracodawcę nawet bez zgody pracownika, którego one dotyczą – leży to w szeroko pojętym prawnie usprawiedliwionym interesie pracodawcy.

Ujawnianie danych służbowych pracownika jest usprawiedliwione obowiązkami i zadaniami jakie leżą po stronie pracodawcy. Pracodawca nie może być pozbawiony możliwości ujawniania nazwisk pracowników, zajmujących określone stanowiska w instytucji. Ma to znaczenie dla kontaktów placówki z czytelnikami, czy kontrahentami i zachowania ciągłości działania jednostki. Dlatego pracodawca jest uprawniony do umieszczania danych pracowników na stronie internetowej, przy drzwiach zajmowanych w bibliotece pokoi, na tabliczkach przy stanowiskach pracy, na identyfikatorach, bez zgody pracownika (analogicznie stażysty, czy zleceniobiorcy). Nie zwalnia to z obowiązku wypełnienia rzetelnego obowiązku informacyjnego, gdyż takie działanie wpływa na zwiększenie kręgu odbiorców danych.

VIII. Podstawy prawne udostępniania danych pracownika.

W odniesieniu do przepisów Kodeksu pracy na bibliotece, jako pracodawcy ciąży obowiązek kierowania pracowników na badania profilaktyczne przed rozpoczęciem pracy oraz w trakcie zatrudnienia (badania okresowe i kontrolne), a także przechowywania wydanych skierowań na badania oraz orzeczeń lekarskich. Sposób kierowania pracownika na w/w badania reguluje rozporządzenie w sprawie przeprowadzania badań lekarskich pracowników, zakresu profilaktycznej opieki zdrowotnej nad pracownikami oraz orzeczeń lekarskich wydawanych do celów przewidzianych w Kodeksie pracy. ADO, czyli pracodawca kierujący pracowników na badania lekarskie nie zawiera umowy powierzenia danych z podmiotem świadczącym usługi z zakresu medycyny pracy. Każdy z administratorów działa w oparciu o przepisy prawa, które odpowiednio regulują obowiązek skierowania na badania i obowiązek przeprowadzenia badań. Dla pracodawcy istotne jest wydanie pracownikowi orzeczenia lekarskiego przez lekarza medycyny pracy, ponieważ jest do tego zobligowany poprzez przepisy Kodeksu pracy. Pracodawca nie ma wglądu w dokumentację medyczną pracownika i nie może żądać od podmiotu leczniczego ich okazania. Pracodawca udostępnia zatem dane pracownika wyłącznie w takim w zakresie jaki nakładają na niego przepisy w związku z wystawieniem skierowa-

nia na badania, przy czym zakres danych jest ograniczony do tych, które są wymagane przepisami prawa. Wzór skierowania na badania został określony w przepisach i pracodawca nie ma swobody w decydowaniu, o tym jakie dane udostępni.

Regulacje prawne dotyczące wymiany informacji pomiędzy pracodawcą a związkiem zawodowym są wskazane w ustawie o związkach zawodowych. Ustawa nie zawiera wyczerpujących regulacji co do zakresu i sposobu udostępniania danych, które pracodawca może wymieniać ze związkami zawodowymi. Związki zawodowe nie mają obowiązku prawnego przekazywania pracodawcy danych osobowych pracowników znajdujących się pod ich ochroną. Odstępstwem jest sytuacja, kiedy pracodawca zamierza rozwiązać umowę o pracę z konkretnym pracownikiem, więc przekazuje niezbędne informacje, celem konsultacji ze związkiem zawodowym.

W przypadku przetwarzania danych osobowych przy gromadzeniu dokumentacji powypadkowej koniecznej do uzyskania jednorazowego odszkodowania przez poszkodowanego pracownika mają zastosowanie odpowiednio przepisy:

- Kodeksu pracy,
- ustawy o ubezpieczeniu społecznym z tytułu wypadków przy pracy i chorób zawodowych,
- rozporządzenia w sprawie szczegółowych zasad orzekania o stałym lub długotrwałym uszczerbku na zdrowiu, trybu postępowania przy ustalaniu tego uszczerbku oraz postępowania i wypłatę jednorazowego odszkodowania,
- rozporządzenia w sprawie ustalenia okoliczności i przyczyn wypadków przy pracy.

Wypadek przy pracy to sytuacja, która wymaga skompletowania szeregu dokumentów, koniecznych do uzyskania jednorazowego odszkodowania przez poszkodowanego pracownika. Najważniejszym z nich jest protokół powypadkowy. W postępowaniu powypadkowym przetwarzane są dane osobowe nie tylko osoby, która uległa wypadkowi. Podczas ustalania przyczyn i okoliczności wypadku brane są również pod uwagę zeznania świadków zdarzenia. Przepisy regulujące postępowanie powypadkowe nie zawierają wytycznych związanych z przetwarzaniem danych osobowych świadków zdarzenia. W związku z powyższym świadkowie zdarzenia muszą wyrazić zgodę na przetwarzanie ich danych osobowych. Dane osobowe świadka zdarzenia zostaną ujęte w protokole w zakresie niezbędnym do prowadzenia postępowania i które mogą być użyteczne np. w ramach sporu sądowego. Zgoda musi być wyrażona dobrowolnie, a świadek poinformowany o możliwości jej wycofania. Przetwarzanie danych osobowych poszkodowanego nie wymaga jego zgody, gdyż odbywa się zgodnie z przepisami prawa.

Jednorazowe odszkodowanie przysługuje ubezpieczonemu, który doznał stałego lub długotrwałego uszczerbku na zdrowiu. Celem jego uzyskania, zgodnie z wymogami prawa, do ZUS należy przesłać szereg dokumentów między innymi protokół powypadkowy, kartę wypadku, zaświadczenie o stanie zdrowia wydane przez lekarza, pod którego opieką, znajduje się poszkodowany, decyzję o stwierdzeniu choroby zawodowej. Z uwagi na fakt, że postępowanie o wypłatę odszkodowania wszczyna się na wniosek poszkodowanego pracownika, zgodnie z przepisami obowiązującego prawa, na gruncie przepisów RODO nie jest wymagana jego zgoda na przetwarzanie danych osobowych.

3.2. Upoważnianie pracowników do przetwarzania danych osobowych oraz prowadzenie ewidencji upoważnień.

W obowiązującej Ustawie ODO nie zostały zawarte zapisy dotyczące upoważnień dla osoby przetwarzającej dane osobowe. Natomiast w art. 29 RODO odniesiono się do tej kwestii w następujący sposób: „Podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub

podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego". Konieczność upoważniania wydaje się także wynikać z obowiązku zapewniania rozliczalności danych. Jednakże obowiązek upoważniania nie został w tych przepisach wskazanych wprost. Nie wskazano w nich także, by koniecznym było wydawanie pisemnych upoważnień, a jedynie, że wszelkie przetwarzania danych osobowych są dopuszczalne wyłącznie za zgodą i na wyraźne polecenie ADO. Zarówno wobec upoważnienia jak i polecenia, nie została określona forma (pisemna czy ustna).

Jednakże ustawodawca odniósł się do problematyki obligowania do zachowania poufności oraz upoważniania do przetwarzania danych osobowych w Ustawie wdrażającej RODO. Na mocy przepisów tej ustawy pracodawcy zostali zobligowani do nadawania pisemnych upoważnień do przetwarzania danych szczególnych kategorii w celach związanych z rekrutacją oraz zatrudnieniem, a także przyznawaniem świadczeń z ZFŚS. Należy zatem uznać, że w celach dowodowych właściwym jest dokumentowanie wszelkich upoważnień, nie tylko tych, których nadanie jest obowiązkiem wynikającym wprost z przepisów prawa. Mając na uwadze fakt najbardziej precyzyjnego określenia zakresu upoważnienia do przetwarzania danych osobowych, by zminimalizować ryzyko dopuszczenia danej osoby do przetwarzania danych, do których dostępu mieć nie powinna, preferuje się określenie zakresu upoważnienia poprzez wskazanie zbiorów danych lub czynności przetwarzania, do których osoba upoważniona powinna mieć dostęp i wszystkich z nimi związanych czynności przetwarzania. Naruszenie zakresu upoważnienia powoduje skutki zarówno wobec upoważnionego, jak i wobec udzielającego upoważnienia.

W praktyce, jeżeli administrator danych powierzy dane osobowe podmiotowi przetwarzającemu, a podmiot ten korzysta jeszcze z dalszych usług firm zewnętrznych, to firmy te mogą być podmiotami przetwarzającymi jak również osobami działającymi z upoważnienia procesora. Jeżeli do przetwarzania danych w imieniu procesora są dopuszczone zleceniobiorcy, w tym przedsiębiorcy, to przyjętą praktyką jest upoważnianie do przetwarzania danych osób, które wykonują zlecenie w siedzibie administratora z wykorzystaniem jego sprzętu i infrastruktury, czyli jak inni pracownicy. W przypadku zleceniobiorców świadczących usługi zewnętrzne wymagające przetwarzania danych, zasadne jest zawarcie umowy powierzenia danych. Upoważnienia powinni otrzymać także wszyscy praktykanci i stażyści, jeżeli będą mieli dostęp (w tym wgląd) do danych osobowych, np. będą porządkować dane w bazie lub niszczyć dokumenty. Przed podjęciem ostatecznej decyzji, należy dokładnie przeanalizować wszystkie okoliczności co do prawnego usankcjonowania dalszego powierzenia. Biorąc pod uwagę fakt, że osoba prowadząca własną działalność ma więcej swobody i ma mniejszy stopnień podporządkowania, słusznym jest podpisanie umowy powierzenia celem większego zabezpieczenia interesów biblioteki. W przypadku powierzenia danych osobowych podmiotowi przetwarzającemu, ten nadając upoważnienia osobom zatrudnionym przy przetwarzaniu powierzonych danych winien zobowiązać ich do zachowania tajemnicy.

Z dokumentacji dotyczącej ochrony danych osobowych obowiązującej w bibliotece powinno jednoznacznie wynikać, kto ma prawo upoważniać pracowników do przetwarzania danych osobowych oraz procedura nadawania/zmiany i odwoływania upoważnień. Do przetwarzania danych mogą zostać dopuszczone tylko i wyłącznie osoby, które otrzymały upoważnienie od osoby działającej w imieniu Administratora (tzn. w bibliotece publicznej dyrektora, a w jednostce wojskowej dowódcę) lub uprawnionej przez niego osoby (np. na podstawie pełnomocnictwa). Sposoby nadawania upoważnień powinny zostać szczegółowo opisane w dokumentacji ochrony danych obowiązującej w instytucji. Każda osoba musi mieć nadane przez ADO upoważnienie do przetwarzania danych osobowych przed przystąpieniem do pracy z danymi osobowymi. Ten obowiązek dotyczy również pracowników już zatrudnionych, wolontariuszy, stażystów, praktykantów. Określenie zakresu przetwarzania danych osobowych może w instytucji należeć do obowiązków kierowników poszczególnych komórek organizacyj-

nych lub bezpośredniego przełożonego, którzy przygotują wniosek o upoważnienie do przetwarzania danych, dopuszczalne jest także wskazanie zakresu upoważnienia, jako zgodnego z zakresem obowiązków pracownika, o ile został on określony dostatecznie szczegółowo. Po przedstawieniu wniosku odpowiednio dyrektorowi, dowódcy jednostki lub innej uprawnionej przez ADO osobie i jego zatwierdzeniu, staje się pełnoprawnym upoważnieniem do przetwarzania danych. Upoważnienie jest nadawane przed przystąpieniem do przetwarzania danych oraz po odbyciu szkolenia w zakresie przepisów o ochronie danych osobowych. Procedura nadawania upoważnień może przewidywać, że upoważnienie do przetwarzania danych osobowych wygasa automatycznie w dniu ustania stosunku pracy, lub zakończenia umowy dotyczącej stażu, wolontariatu, czy praktyk. Nadrzędnym zadaniem jest prawidłowe przypisanie uprawnień osobom upoważnionym, właściwe nadanie upoważnień i sprawowanie kontroli w związku z przetwarzaniem danych, np. poprzez prowadzenie rejestru upoważnień. Wzór upoważnienia winien stanowić załącznik do obowiązującej w jednostce dokumentacji ochrony danych. Oryginały upoważnień winny być przechowywane w aktach osobowych w dziale kadr biblioteki, kopie w/w dokumentów winien gromadzić IOD – taki podział nie jest obowiązkiem, ale stanowi dobrą, często praktykowaną przez biblioteki zasadę. Dobrą praktyką jest przekazanie kopii upoważnienia osobie upoważnionej. Jedynie osoby posiadające nadane przez administratora upoważnienia są uprawnione do przetwarzania danych w zakresie ustalonym w tym dokumencie, w tym do otrzymania dostępu do systemów służących do przetwarzania danych. Przetwarzanie danych bez upoważnienia stanowi naruszenie przepisów o ochronie danych osobowych.

Korzystnym z punktu widzenia biblioteki jest ewidencjonowanie upoważnień. Nie wynika ono z przepisów prawa. Prowadzenie rejestru jest dobrowolną praktyką wprowadzoną przez jednostki. O jego prowadzeniu stanowi zwykle zapis w obowiązującej dokumentacji dotyczącej ochrony danych (np. polityce bezpieczeństwa informacji), celem sprawowania efektywnej kontroli nad przetwarzaniem danych osobowych. Każde nowe upoważnienie, bądź dokonane w nim zmiany powinny zostać odnotowane w ewidencji. Sprawdzonym rozwiązaniem jest prowadzenie ewidencji przez IOD w formie elektronicznej, np. w arkuszu kalkulacyjnym. Inspektor, który prowadzi rejestr, odnotowuje do jakich czynności przetwarzania upoważniony jest pracownik w ramach poszczególnych zbiorów danych lub czynności przetwarzania. Decyzją dyrektora jest określany zakres informacji zawartych w ewidencji. Bez wątpienia przydatne są następujące informacje: imię i nazwisko osoby upoważnionej, nazwy zbiorów/czynności przetwarzania, do których nadane jest upoważnienie, data nadania, zmiany, odwołania, zakres upoważnienia, nazwa systemu, w którym przetwarzane są dane oraz login użytkownika systemu. Jeżeli przyjęto rozwiązanie w postaci nadawania upoważnień w zakresie zgodnym z zakresem obowiązków, powinien on być znany i wskazany w ewidencji, ponieważ na jego podstawie będzie możliwa kontrola uprawnień takiej osoby. W takim wypadku zalecane jest wprowadzenie odrębnego dokumentu określającego zakres uprawnień do systemów informatycznych, gdyż wskazane odwołanie do zakresu obowiązków może być niewystarczające. W ewidencji na bieżąco aktualizuje się faktyczny stan nadanych w bibliotece upoważnień.

3.3. Zobowiązanie pracowników do zachowania poufności.

Zasada poufności to jedna z najważniejszych zasad zawartych w przepisach RODO, jak również w przepisach prawa, normach i innych dokumentach, które stały się źródłem przepisów rozporządzenia. Warto pamiętać, że każdy pracownik zatrudniony w Polsce na umowę o pracę jest zgodnie z art. 100 Kodeksu pracy „obowiązany wykonywać pracę sumiennie i starannie oraz stosować się do poleceń przełożonych, które dotyczą pracy, jeżeli nie są one sprzeczne z przepisami prawa lub

umową o pracę" oraz „dbać o dobro zakładu pracy, chronić jego mienie oraz zachować w tajemnicy informacje, których ujawnienie mogłoby narazić pracodawcę na szkodę". Niezależnie więc od tego, czy pracownik zobowiąże się w inny, dodatkowy sposób do zachowania poufności, ma taki obowiązek zgodnie z przepisami prawa. W przypadku bibliotek warto rozważyć również inne formy takiego zobowiązania, co wynika z kilku czynników.

Przede wszystkim, przy zachowaniu poufności kluczowe znaczenie będzie miała postawa i świadomość pracowników bibliotek. W większość bibliotek pracuje wykwalifikowana kadra, która rzetelnie podchodzi do swoich obowiązków. Warto jednak pamiętać, że przy dużej liczbie bibliotek w Polsce statystycznie w niektórych z nich mogą się również pojawić pracownicy nieodpowiedzialni. Zdarzają się również sytuacje, w których pracownicy bibliotek rzetelnie wykonują swoje obowiązki wynikające z zakresu zadań, jednak bagatelizują kwestię ochrony danych osobowych i nie poczuwają się do odpowiedzialności, jaka została na nich nałożona. Takie sytuacje są niebezpieczne, ponieważ biblioteki realizują szczególną misję i powinny systematycznie budować dobry, godny zaufania wizerunek. Jednocześnie warto pamiętać, że wysoka świadomość pracowników w zakresie ochrony danych osobowych prowadzi do tego, że wykonują oni swoje zadania uważniej i popełniają mniej błędów. Jednym z narzędzi, które przyczyniają się do zabezpieczenia interesu biblioteki jako ADO i motywowania pracowników biblioteki do zwrócenia szczególnej uwagi na przetwarzanie danych osobowych jest zobowiązanie pracowników do zachowania poufności.

W celu uporządkowania tego obszaru warto zwrócić uwagę, że w praktyce funkcjonują cztery rozwiązania prawne w tym zakresie:

- nadawanie pracownikowi biblioteki pisemnego upoważnienia do przetwarzania danych osobowych (opisane w podrozdziale 3.2.), na którym znajduje się zobowiązanie pracownika do zachowania poufności, które pracownik kwituje własnoręcznym podpisem,
- opracowanie wzoru oświadczenia pracownika, w którym oświadcza, że zapoznał się z dokumentacją bezpieczeństwa ochrony danych osobowych i jednocześnie zobowiązuje się do zachowania poufności, które pracownik kwituje własnoręcznym podpisem,
- wpisanie i doprecyzowanie kwestii zachowania poufności przez pracowników w umowie o pracę,
- sporządzenie osobnej umowy o zachowanie poufności (rozwiązanie rekomendowane dla współpracowników biblioteki, którzy nie są zatrudnieni na umowę o pracę).

Poprzez przepisy RODO nikt nie narzuca bibliotece zastosowania konkretnego rozwiązania. Decyzja dotycząca wyboru i zastosowania optymalnego zobowiązania pracowników do zachowania poufności zawsze należeć będzie do ADO, czyli w praktyce funkcjonowania biblioteki będzie ją musiał ostatecznie podjąć dyrektor biblioteki, a w przypadku biblioteki wojskowej dowódca jednostki. Niezależnie od tego, czy zobowiązanie znajdzie się na druku upoważnienia, czy też na druku oświadczenia pracownika o zapoznaniu się z dokumentacją, najważniejsze jest przede wszystkim to, żeby nie zapomnieć o możliwości przyjęcia takiej formy zabezpieczenia danych osobowych i interesów biblioteki. Istnieje wysokie prawdopodobieństwo, że takie działanie przyczyni się do zwiększenia świadomości pracowników instytucji w zakresie ochrony danych osobowych. A w przypadku naruszenia bezpieczeństwa danych osobowych szybciej i bardziej efektywnie będzie można określić zakres odpowiedzialności pracownika, który jest sprawcą naruszenia.

Jednym ze wskazanych wyżej rozwiązań jest podpisanie odrębnej umowy o zachowanie poufności. Takie rozwiązanie jest szczególnie rekomendowane, jeżeli ADO nawiązuje współpracę z osobą fizyczną i taka osoba nie jest zatrudniona na umowę o pracę (zostaje podpisana umowa cywilnoprawna). Wówczas dyrektor biblioteki (odpowiednio dowódca jednostki) szczególnie powinien rozważyć podpisanie umowy o zachowanie poufności z kilku względów, m.in.:

- taki współpracownik nie podlega przepisom ustawy Kodeks pracy w zakresie wskazanego wcześniej art. 100, czyli nie jest zobowiązany do zachowania poufności poprzez przepis prawa,
- taki współpracownik nie zna wewnętrznych regulacji odnoszących się do ochrony danych osobowych w bibliotece, nie bierze również udziału w szkoleniach organizowanych dla etatowych pracowników,
- nie ma możliwości podpisania tzw. „umowy powierzenia danych osobowych" z osobą fizyczną, która nie prowadzi działalności gospodarczej (więcej na ten temat w podrozdziale 5.1.).

Przy podejmowaniu decyzji w zakresie podpisania odrębnej umowy poufności ze współpracownikiem warto kierować się przede wszystkim zdrowym rozsądkiem. Można oczywiście przyjąć stałą praktykę, że każdy kto podpisuje umowę cywilnoprawną z biblioteką podpisuje również umowę poufności. Nie ulega jednak wątpliwości, że bardziej zasadne jest podpisanie takiej umowy z zewnętrznym informatykiem, który podczas wykonywanych zadań ma dostęp do wielu danych, niż np. z bohaterem spotkania autorskiego, który nie przetwarza danych osobowych lub nie robi tego na dużą skalę. Kwestii zachowania poufności przez pracowników biblioteki nie należy w żaden sposób bagatelizować. Praktyka funkcjonowania bibliotek wskazuje bowiem na przykłady niezachowania poufności, które wiązały się z realnym naruszeniem praw i wolności osób fizycznych. Były to zdarzenia w skali mikrostrukturalnej, kiedy np. pracownik biblioteki w małej miejscowości opowiedział sąsiadom o tym, jakie książki wypożycza nowy mieszkaniec, zdradzając w ten sposób jego poglądy filozoficzne i religijne (szczególne kategorie danych). Zdarzały się również naruszenia poufności na szeroką skalę, prowadzące do popełnienia przestępstwa, np. wyłudzanie kredytów na dane czytelników biblioteki w jednym z miast województwa lubelskiego. W tym konkretnym przypadku w latach 2014-2015 poszkodowanych zostało ponad dziewięćdziesiąt osób.

3.4. Odpowiedzialność pracowników w związku z przetwarzaniem danych osobowych.

Jak wskazano wcześniej, pracownik dopuszczany do przetwarzania danych osobowych musi mieć nadane upoważnienie do wykonywania czynności z danymi. Upoważnienie jest nadawane przez ADO i powinno określać w szczególności zakres dostępu do danych, a także czas na jaki zostało ono nadane. Zakres przetwarzanych danych może być także określony w innych dokumentach, np. w zakresie obowiązków pracownika.

Wraz z nadaniem upoważnienia pracownik nabywa kilka istotnych obowiązków. Po pierwsze musi przetwarzać dane zgodnie z obowiązującymi u ADO regulaminami i procedurami oraz zachować w tajemnicy zarówno dane osobowe jak i sposoby zabezpieczenia tychże danych (więcej na temat zachowania poufności w podrozdziale 3.3.). Obowiązek tajemnicy dotyczy w takim samym zakresie danych, do których przetwarzania jest upoważniony, jak i tych, w których posiadanie wszedłby przypadkiem, np. w związku z naruszeniem. Po drugie, wykorzystanie danych jest możliwe wyłącznie do celów służbowych. Po trzecie pracownik ma dbać o powierzone mu zasoby służące do przetwarzania danych, w tym przede wszystkim zasoby informatyczne. Ostatnią kwestią, lecz równie ważną, jest obowiązek niezwłocznego zgłaszania wszelkich nieprawidłowości i naruszeń związanych z przetwarzaniem danych osobowych do ADO i IOD-a.

W związku z powyższymi obowiązkami pracownik ponosi także pełną odpowiedzialność za stosowanie wzmiankowanych procedur i regulaminów w procesach przetwarzania danych osobowych, w których bierze udział. Procesy przetwarzania są na bieżąco kontrolowane przez IOD.

W przypadku, gdy zostaną wykryte nieprawidłowości lub zaniechania związane z przetwarzaniem danych, IOD ze wsparciem ADO przeprowadza postępowanie wyjaśniające mające na celu ustalenie okoliczności i zakres ewentualnego naruszenia. Jeśli w wyniku postępowania zostanie stwierdzona odpowiedzialność pracownika, ADO może wyciągnąć wobec takiego pracownika konsekwencje adekwatne do wagi stwierdzonych nieprawidłowości lub zaniechań. Wszystkie konsekwencje służbowe wobec pracownika będą miały oparcie w Kodeksie pracy. W skrajnych przypadkach udział pracownika w weryfikowanym naruszeniu może być potraktowany jako ciężkie naruszenie obowiązków pracowniczych. ADO może także żądać pokrycia wyrządzonych szkód przez pracownika zgodnie z zasadami określonymi w obowiązujących przepisach prawa - w przypadku działania nieumyślnego, odszkodowanie może mieć wysokość maksymalną do trzech miesięcznych pensji, zaś w przypadku działania umyślnego odszkodowanie może mieć pełną wysokość wyrządzonej szkody.

Oczywiście konsekwencje dyscyplinarne nie wykluczają odpowiedzialności karnej pracownika zgodnie z Ustawą ODO oraz możliwości wniesienia przez ADO sprawy do sądu powszechnego z powództwa cywilnego o zrekompensowanie poniesionych strat.

3.5. Szkolenia pracowników.

Jednym z istotnych działań mających na celu zapewnienie prawidłowego stosowania przepisów RODO w bibliotece są szkolenia pracowników. Podobnie jak w przypadku wielu innych aspektów ochrony danych osobowych, w przepisach RODO i normach zawartych w innych aktach prawnych nie ma precyzyjnych wytycznych dotyczących przeprowadzania takich szkoleń. Twórcy przepisów RODO ograniczyli się do wskazania w art. 39 ust. 1 lit. b, że do zadań IOD należą m.in. „działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty". Przepis ten nie zdejmuje jednak odpowiedzialności z ADO, szczególnie z kadry kierowniczej biblioteki w zakresie dbałości o posiadanie przez pracowników kompetencji do prawidłowego przetwarzania danych osobowych.

Najczęściej występującym w bibliotekach dylematem jest to, z jaką częstotliwością powinny odbywać się szkolenia dla pracowników. Biorąc pod uwagę systematyczne nowelizacje aktów normatywnych, które mają realny wpływ na ochronę danych osobowych w podmiotach publicznych, rozsądną i adekwatną propozycją jest przyjęcie zasady, że każdy pracownik powinien zostać przeszkolony co najmniej raz w roku. Warto też zaznaczyć, że jeżeli dochodzi do poważnych zmian legislacyjnych to jest to naturalny sygnał, że nie warto czekać z organizacją kolejnego szkolenia. ADO musi także zadbać o to, aby przeszkolony został każdy nowy pracownik biblioteki. Nikt nie powinien przetwarzać danych osobowych bez odpowiedniego przygotowania i zaznajomienia z obowiązującymi w bibliotece procedurami. Częstotliwość prowadzonych szkoleń powinna także wynikać z naruszeń bezpieczeństwa danych osobowych oraz skarg, jakie osoby korzystające z usług biblioteki składają do IOD oraz – przede wszystkim – do Prezesa Urzędu Ochrony Danych Osobowych. Jeżeli w bibliotece występują realne problemy z bezpieczeństwem danych to warto przeprowadzać więcej szkoleń.

Dyrektor biblioteki musi realnie ocenić możliwości IOD w zakresie prowadzenia szkoleń dla pracowników. Jeżeli jest to osoba zatrudniona w bibliotece, wykonująca obowiązki IOD od niedawna i jako dodatkowe do codziennych obowiązków, która nie czuje się jeszcze na siłach, żeby przeprowadzić zajęcia szkoleniowe dla pracowników biblioteki, warto rozpocząć od skierowania takiego IOD na szkolenia, kursy, konferencje, czy studia podyplomowe. Wówczas, w przyszłości inspektor będzie mógł podzielić się zdobytą wiedzą ze współpracownikami. Jest to lepsze rozwiązanie, niż zmuszanie go do prowadzenia szkolenia, ponieważ wówczas może udzielić współpracownikom błędnych informacji, bądź też nie odpowiedzieć na zadawane przez nich pytania. W takiej sytuacji warto rozważyć

wynajęcie trenera zewnętrznego. Taka osoba oprócz udokumentowanych kwalifikacji powinna przede wszystkim posiadać doświadczenie we współpracy z bibliotekami i znać ich specyfikę.

Szkolenia dla pracowników mogą mieć różne formy. Niektórzy preferują tradycyjne zajęcia grupowe dla wszystkich pracowników biblioteki. Mocną stroną takiego rozwiązania jest możliwość spotkania całego zespołu, wymiany doświadczeń i skupienia się na zagadnieniach związanych z ochroną danych osobowych, które często są odkładane z powodu innych pilnych zadań. Bardzo ważne jest, żeby szkolenie przebiegało w atmosferze, która sprzyja zadawaniu prowadzącemu pytań i omawianiu realnych problemów w konkretnej instytucji. Warto, żeby odpowiedzi na pytania były udzielane podczas szkolenia (a nie np. podczas przerw indywidualnie), wówczas mogą z nich skorzystać wszyscy pracownicy. Inną formą są szkolenia internetowe polegające na przekazywaniu informacji i weryfikowaniu zdobytej wiedzy. Takie rozwiązanie stosuje się najczęściej w bibliotekach, w których jest zatrudniona duża liczba pracowników. Nie powinno jednak być tak, że w bibliotece odbywają się wyłącznie szkolenia internetowe. Można jednak przyjąć, że jeżeli w danym roku odbyło się szkolenie w formie tradycyjnej, a w kolejnym nie doszło do znaczącej zmiany przepisów prawa, to może się odbyć szkolenie przez Internet.

W niektórych bibliotekach są zatrudnieni tzw. „zewnętrzni" IOD, którzy świadczą takie usługi indywidualnie lub w ramach prowadzonej działalności gospodarczej. Na rynku istnieją też przedsiębiorstwa, które świadczą kompleksowe usługi w zakresie ochrony danych osobowych dla bibliotek, a ich pracownicy pełnią w bibliotekach funkcję IOD. Bardzo często biblioteki mają problem z wyegzekwowaniem świadczenia takich usług na odpowiednim poziomie. Dlatego bardzo ważne jest, aby już na etapie podpisywania umowy z taką firmą zastrzec, że ADO oczekuje przeprowadzania regularnych szkoleń dla pracowników i wskazać tę częstotliwość, np. raz w miesiącu dla nowych pracowników, zleceniobiorców, praktykantów, stażystów, a także raz lub dwa razy do roku dla stale zatrudnionych. Jeżeli umowa jest już podpisana i nie znalazły się takie precyzyjne zapisy, to IOD i tak musi się wywiązać z przeprowadzania szkoleń, ponieważ taki obowiązek nakładają na niego wskazane na początku podrozdziału przepisy RODO i nie jest to zagadnienie uznaniowe. Zawsze jednak warto dojść z IOD do porozumienia i wypracować rozwiązanie, w którym taka osoba nie będzie realizowała szkoleń w minimalnym stopniu, np. tylko w skróconej formie przez Internet. IOD zawsze może sugerować takie rozwiązanie, ponieważ tak jak wskazano na początku podrozdziału, w przepisach RODO nie doprecyzowano, ile szkoleń i w jakiej formie powinno się odbywać w bibliotece.

Sama metodyka szkoleń i ich zakres merytoryczny zależy od wielu czynników, m.in.:

- Poziomu wiedzy pracowników biblioteki w zakresie ochrony danych osobowych,
- liczby pracowników,
- liczby czytelników,
- zakresu działalności,
- naruszeń, skarg i innych incydentów, jakie do tej pory miały miejsce.

Warto jednak zwrócić szczególną uwagę na to, aby szkolenia miały jak najwięcej walorów praktycznych. Zagadnienia teoretyczne, zakres podmiotowy i przedmiotowy uregulowań prawnych oraz definicje i podziały powinny zostać ograniczone do niezbędnego minimum. Większość pracowników biblioteki potrzebuje praktycznych informacji w jaki sposób przetwarzać dane osobowe podczas wykonywania codziennych czynności w pracy, aby zapewnić ich bezpieczeństwo i postępować zgodnie z przepisami RODO. Z uwagi na to, że prezentowane podczas szkoleń zagadnienia są trudne, szczególnie dla osób, które nie miały wcześniej do czynienia z ochroną danych osobowych, warto urozmaicać takie szkolenia aktywizującymi metodami dydaktycznymi, np. przygotowując ćwiczenia powtórzenia z udziałem interaktywnych quizów, bądź też dzieląc uczestników na grupy, które będą ze sobą rywalizowały. Takie rozwiązania zwiększają zainteresowanie uczestników i pomagają im przyswoić więcej merytorycznej wiedzy.

Do rozstrzygnięcia pozostaje jeszcze jeden dylemat, przed którym stoją osoby zarządzające bibliotekami. W niektórych instytucjach zorganizowano szkolenia dotyczące stosowania przepisów RODO, prowadzone przez profesjonalnych trenerów zewnętrznych, które odbyły się przed 25 maja 2018 r. (np. w 2017 r.). Pojawiło się pytanie, czy nie należy jak najszybciej ponownie zorganizować takich szkoleń, ponieważ bardzo wiele wytycznych, informacji, jak również uregulowań prawnych pojawiło się później, kiedy już RODO bezwzględnie obowiązywało. Przede wszystkim warto podkreślić, że takie szkolenia były potrzebne i najważniejsze przepisy funkcjonowały tak naprawdę jeszcze dwa lata przed tą datą. Oczywiście nie należy bagatelizować późniejszego wejścia w życie nowej polskiej Ustawy ODO, rozpoczęcia działalności nowego Prezesa Urzędu Ochrony Danych Osobowych i wydawania przez niego decyzji, jak również publikowania wytycznych. Jednak zasadnicza konstrukcja systemu ochrony danych osobowych była znana wcześniej i im wcześniej pracownicy biblioteki zostali zaznajomieni z nowymi regulacjami, tym więcej mieli czasu, żeby się do nich przygotować. Warto oczywiście organizować kolejne szkolenia zarówno prowadzone przez IOD, jak i trenerów zewnętrznych, jednak powinny być one kontynuacją dotychczasowego wdrażania zmian w ochronie danych osobowych.

Poza szkoleniami warto zachęcać pracowników do samodzielnego poszerzania swojej wiedzy na temat ochrony danych osobowych. Bardzo przydatne w tym zakresie są strony internetowe, książki i czasopisma poświęcone tej problematyce. Przy podejmowaniu decyzji o prenumeracie periodyku, z którego pracownicy będą mogli czerpać wiedzę na temat wdrażania przepisów RODO warto zwrócić uwagę, aby było to czasopismo, w którym takie zagadnienia omawiane są pod kątem bibliotek. Analogicznie warto podejść do kwestii zakupu literatury, sięgając po pozycje przydatne z punktu widzenia funkcjonowania bibliotek.

3.6. Dobre praktyki, wytyczne i wskazówki.

Zobowiązanie do zachowania poufności

Oświadczam, że zapoznałem/am się z zasadami zachowania danych osobowych w poufności obowiązującym w ..... i zobowiązuję się do ich przestrzegania oraz zachowania wszelkich informacji chronionych, do których otrzymam dostęp, w poufności.

Zostałem/am również zapoznany/a z ogólnymi zasadami zabezpieczenia i przetwarzania danych osobowych wynikającymi z RODO i zobowiązuję się do ich przestrzegania. Oświadczam, że zachowam w poufności wszelkie informacje chronione, które przetwarzałem/am lub przetwarzam w ramach wykonywanych obowiązków/umowy/usług oraz metody ich zabezpieczeń, także po ustaniu wykonywania zlecenia/umowy/świadczenia pracy.

Jestem świadomy/a, że naruszenie poufności danych lub wykorzystanie ich w innym celu/zakresie niż wskazany w upoważnieniu do przetwarzania danych, w szczególności do osiągnięcia korzyści własnych lub innych podmiotów, może skutkować odpowiedzialnością karną, dyscyplinarną lub odszkodowawczą na rzecz administratora danych i/lub pokrzywdzonych na skutek mojego działania osób.

Przykładowa zgoda na opublikowanie wizerunku pracownika na stronie internetowej wraz z obowiązkiem informacyjnym

Wyrażam zgodę na nieodpłatne rozpowszechnianie mojego wizerunku przez **[dane administratora/pracodawcy, tzn. pełna nazwa, dane kontaktowe]** na stronie internetowej pracodawcy w celu promocji jego pozytywnego wizerunku, bieżącej działalności, w tym produktów i usług. Zostałem/am poinformowany/a, że zgodę mogę wycofać w dowolnym momencie i jest ona dobrowolna. Jestem świadomy/-a, iż z tytułu wykorzystania mojego wizerunku i udzielenia powyższej zgody otrzymam dodatkowego wynagrodzenia.

Imię i nazwisko:.....
Data i podpis pracownika: .....

Informacja o zasadach przetwarzania danych zgodnie z art. 13 RODO

1. Administratorem Pani/a danych osobowych jest [**należy podać dane administratora/, w tym dane kontaktowe]**
2. Administrator wyznaczył inspektora, z którym można się skontaktować w sprawach związanych z przetwarzaniem danych osobowych **[należy podać dane kontaktowe]**
3. Pani/a dane osobowe będą przetwarzane na stronie internetowej pracodawcy w celu promocji jego pozytywnego wizerunku, bieżącej działalności, w tym produktów i usług na podstawie wyrażonej zgody (art. 6 ust. 1 lit. a RODO). Zgoda może zostać odwołana w dowolny momencie, bez wpływu na przetwarzanie, które miało miejsce do momentu wycofania. W celu wycofania zgody należy skontaktować się z IOD.
4. Odbiorcami Pani/a danych osobowych będą podmioty upoważnione do tego na podstawie przepisów prawa, a także **[należy wskazać innych odbiorców, np. podmiot zapewniający poprawne działanie strony internetowej, osoby korzystające ze strony internetowej, w tym klienci i kontrahenci]**
5. Dane będą przetwarzane do momentu wycofania zgody lub ustania celu przetwarzania, w szczególności ze względu na ustanie stosunku pracy.
6. Ma Pan/i prawo żądania od administratora dostępu do swoich danych, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub wniesienia sprzeciwu wobec przetwarzania, a także do przenoszenia danych na podstawie i zgodnie z art. 15-22 RODO.
7. Ma Pan/i prawo wniesienia skargi na sposób przetwarzania przez administratora do Prezesa UODO (uodo.gov.pl)
8. Podanie danych jest dobrowolne, ale niezbędne do opublikowania zdjęcia na stronie internetowej administratora.

Szkolenie z…… w dniu …….
Imię, nazwisko oraz podpis

Administratorem Pani/a danych osobowych jest ..... Dane są gromadzone w związku z udokumentowaniem przeprowadzenia szkolenia, a podstawą do działania jest prawny interes administratora. Podanie danych jest dobrowolne, ale niezbędne do udziału w szkoleniu. Pani/a dane nie będą udostępniane innym podmiotom. Przysługuje Pani/u prawo wglądu, edycji, ograniczenia przetwarzania i wniesienia sprzeciwu na dalsze przetwarzanie, a także prawo wniesienia skargi na proces przetwarzania do Prezesa UODO. Dane będą przetwarzane do ..... lat po zakończeniu szkolenia.

4 PRZETWARZANIE DANYCH OSOBOWYCH OSÓB KORZYSTAJĄCYCH Z OFERTY BIBLIOTEKI

4.1 Ogólna charakterystyka realizacji praw osób, których dane dotyczą.

Przepisy RODO nakładają na administratorów szerokie spektrum obowiązków związanych z realizacją praw osób, których dane dotyczą. Jednym z najważniejszych jest rzetelnie przekazany obowiązek informacyjny wynikający z art. 13 i 14, który daje osobie korzystającej z usług biblioteki wiedzę o sposobie przetwarzania jej danych. Powinien on być napisany prostym i zrozumiałym językiem i być przekazany w momencie pozyskiwania danych bezpośrednio od osoby, której dane dotyczą, a w przypadku pozyskania danych z innego źródła (np. od innej biblioteki) w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych, przy czym jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej komunikacji z tą osobą. Jeżeli dane mają być ujawnione innym podmiotom (np. w celach promocyjnych urzędowi gminy lub innej bibliotece w związku z zawartym porozumieniem), to informację o udostępnieniu należy przekazać najpóźniej w momencie tego udostępnienia, jednak najlepiej byłoby wskazać te podmioty od razu w pierwotnie realizowanym obowiązku informacyjnym.

I. Kategorie osób wobec których należy realizować obowiązek informacyjny.

Działalność współczesnej biblioteki jest oparta na przetwarzaniu danych osobowych, w szczególności danych czytelników, pracowników, uczestników szkoleń, konkursów, lekcji bibliotecznych i innych wszelkiego rodzaju wydarzeń, które są dokumentowane fotograficznie oraz filmowo. Większość danych osobowych przetwarzanych w bibliotece jest pozyskiwanych bezpośrednio od osób, których dane dotyczą i wobec tych osób, należy realizować obowiązki informacyjne, chyba że i w zakresie w jakim mają one już wiedzę o przetwarzaniu ich danych (art. 13 ust. 4 RODO). Są także sytuacje, w których dane są pozyskiwanie z innego źródła, np. za zgodą czytelnika są one udostępniane z innych bibliotek w związku z zawartymi porozumieniami lub w związku ze wspólnie prowadzonymi działaniami promującymi czytelnictwo. Przepisy art. 14 ust. 5 RODO przewidują wyjątki od konieczności realizacji obowiązków informacyjnych wobec osób, których dane zostały udostępnione bibliotece gdy – i w zakresie, w jakim:

I. osoba, której dane dotyczą, dysponuje już tymi informacjami,
II. udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku; w szczególności w przypadku przetwarzania do celów archiwalnych w interesie

publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1, lub o ile obowiązek, o którym mowa w ust. 1 niniejszego artykułu, może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. W takich przypadkach administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie,

III. pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą, lub

IV. dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.

Jednakże dobrą praktyką jest udostępnianie klauzuli informacyjnej w każdym wypadku.

II. Forma udostępnienia klauzuli informacyjnej.

Administrator może realizować obowiązki informacyjne w dowolnej formie: na piśmie, elektronicznie, a nawet ustnie (ale tylko, gdy wyraźnie zażąda tego osoba, do której kierowane są informacje). Klauzula informacyjna kierowana do czytelników i niezarejestrowanych użytkowników biblioteki może być zawarta w regulaminie biblioteki, z którym jest ta osoba zobowiązana się zapoznać. Atutem tego rozwiązania jest też to, że regulamin zazwyczaj jest zamieszczony na stronie internetowej biblioteki, co daje możliwość zapoznania się z niezbędnymi informacjami w dowolnym momencie. Osoby objęte monitoringiem wizyjnym, powinny mieć możliwość przeczytania klauzuli w siedzibie biblioteki, ale także na stronie internetowej. Uczestnicy szkoleń i wydarzeń powinni być informowani w momencie zapisu lub otrzymania zaproszenia. Cała polityka informacyjna biblioteki powinna być spójna oraz przemyślana. W każdej bibliotece został wyznaczony inspektor ochrony danych, którego rolą jest wsparcie dyrektora w przygotowaniu treści obowiązków informacyjnych, a także w ich realizacji. Coraz więcej podmiotów publicznych, przyjmuje jako dobrą praktykę, zasadę zamieszczania wszelkich klauzul informacyjnych w biuletynie informacji publicznej, w przeznaczonej do tego celu zakładce.

Nie można zmuszać osoby, której dane dotyczą do potwierdzania zapoznania się z przekazaną klauzulą. Jest to jej uprawnienie, a nie obowiązek. Praktyka uzyskiwania obligatoryjnych oświadczeń o zapoznaniu się z klauzulą informacyjną biblioteki jest niezgodna z przepisami RODO.

III. Zakres przekazywanych informacji.

Osobie, której dane dotyczą zgodnie z wymaganiami art. 13 ust. 1 i 2 RODO, należy przekazać bardzo szczegółowe informacje o zasadach przetwarzania jej danych, dodatkowo, jeżeli dane zostały udostępnione z innego źródła, należy osobie, której dane dotyczą przekazać informację o źródle pochodzenia danych, a także kategoriach przetwarzań tych danych (art. 14 ust. 1 i 2 RODO). Warto podkreślić, że w przypadku wielu kategorii danych przetwarzanych w bibliotece kryteria czasu przechowywania danych precyzyjnie określają powszechnie obowiązujące przepisy prawa, na które można powołać się w klauzuli informacyjnej. Dodatkowo, jeżeli w bibliotece został opracowany jednolity rzeczowy wykaz akt, można powołać się na niego i przepisy o narodowym zasobie archiwalnym. W przypadku przetwarzania danych osobowych na podstawie zgody, bardzo ważne jest poinformowanie, że podanie danych jest dobrowolne, a zgoda może zostać odwołana w dowolnym momencie. Osoba, której dane dotyczą musi także znać konsekwencje niepodania danych, np. nie-

możliwe będzie wypożyczenie materiałów bibliotecznych do domu. Co ważne, za każdym razem przekazując klauzulę informacyjną, należy poinformować osobę, której dane będą przetwarzane, o jej ustawowym prawie do złożenia skargi na administratora do Prezesa UODO. Ma to szczególne znaczenie, gdy dane są przetwarzane przez podmiot publiczny, gdyż obywatele mogą sądzić, że skoro przetwarzanie ich danych osobowych jest realizowane na podstawie ciążącego na podmiocie publicznym obowiązku wynikającego z przepisu prawa, to nie przysługuje im prawo skargi na sposób przetwarzania tych danych.

IV. Inne prawa osób, których dane dotyczą.

Osobie, której dane są przetwarzane w ramach działalności bibliotecznej przysługują także szczególne prawa w zakresie sposobu przetwarzania jej danych przez administratora:

- prawo do uzyskania dostępu do danych (art. 15 RODO),
- prawo do sprostowania danych (art. 16 RODO),
- prawo do usunięcia danych (art. 17 RODO),
- prawo do ograniczenia przetwarzania (art. 18 RODO),
- prawo do przenoszenia danych (art. 20 RODO),
- prawo do wyrażenia sprzeciwu na przetwarzanie danych (art. 21 RODO),
- prawo do nie podlegania zautomatyzowanym decyzjom w tym profilowaniu (art. 22 RODO).

Sposób realizowania tych praw został określony w art. 12 RODO, dodatkowo wskazano w art. 16-18 RODO, że w przypadku zrealizowania prawa do sprostowania, usunięcia lub ograniczenia przetwarzania danych administrator ma obowiązek poinformować o tych działaniach wszystkich odbiorców danych, którym te dane zostały ujawnione, chyba że byłoby to niemożliwe lub wiązało się z niewspółmiernie dużym wysiłkiem (art. 19 RODO). Dyrektor biblioteki po otrzymaniu żądania od osoby, której dane dotyczą ma obowiązek dokonać weryfikacji tożsamości tej osoby. Jeżeli jednoznaczna weryfikacja okaże się niemożliwa, należy odmówić realizacji prawa przysługującego na mocy przepisów RODO, ponieważ mogłoby to doprowadzić do naruszenia praw i wolności osoby, której dane faktycznie dotyczą (art. 12 ust. 6 RODO). Należy podkreślić, że prawa przysługujące na mocy RODO nie przysługują rodzicom pełnoletnich dzieci, chyba że są oni ich ustawowymi opiekunami, ze względu na ograniczoną możliwość decydowania o sobie, np. ze względu na stopień niepełnosprawności. W przypadku małoletnich prawa z art. 15-18 i 20-22 RODO mogą być realizowane wobec obojga rodziców, a także innych ustanowionych opiekunów prawnych.

Punktem kontaktowym dla osób, których dane dotyczą powinien być IOD, do którego pracownicy oraz dyrektor powinni przekazywać otrzymane żądania do zaopiniowania. Realizacja praw podmiotu danych jest wykonywana przez dyrektora biblioteki (odpowiednio dowódcę, rektora uczelni lub inną umocowaną przez administratora osobę), na podstawie otrzymanej od inspektora opinii. Na wykonanie żądania administrator ma miesiąc, chyba że żądanie miałoby skomplikowany charakter, wówczas może ulec przedłużeniu o kolejne dwa miesiące, ale należy poinformować o takim przedłużeniu (art. 12 ust. 3 RODO). Żądanie powinno być realizowane w tej samej formie, w której zostało złożone, w szczególności elektronicznie, chyba że osoba, której dane dotyczą zażąda innej formy. Należy podkreślić, że przy realizacji żądania niezbędne jest zastosowanie tych samych środków zapewniających poufność danych, jak przy każdym innym przetwarzaniu danych w bibliotece, w szczególności dane powinny zostać zaszyfrowane przed wysłaniem, a hasło powinno zostać przekazane inną drogą komunikacji lub być informacją, którą może posiadać tylko osoba, której dane dotyczą, np. może to być numer karty bibliotecznej.

V. Realizacja żądania dostępu do danych (art. 15 RODO).

W ramach dostępu do danych osoba, której dane dotyczą może uzyskać informacje o tym, czy jej dane są przetwarzane, a jeżeli tak, jest jest uprawniona do uzyskania informacji o:

1. celach przetwarzania,
2. kategoriach odnośnych danych osobowych (tych, które zostały udostępnione bibliotece),
3. odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych,
4. planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe, kryteriach ustalania tego okresu (np. poprzez odniesienie do przepisów prawa),
5. prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania,
6. prawie wniesienia skargi do Prezesa UODO,
7. jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle,
8. zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą powinna zostać poinformowana o odpowiednich zabezpieczeniach, o których mowa w art. 46 RODO, związanych z przetwarzaniem jej danych.

Udostępnienie kopii danych osobowych na zasadach określonych w art. 15 ust. 3 RODO nie oznacza, że ADO ma obowiązek udostępnić kopie wszystkich posiadanych dokumentów (papierowych i elektronicznych). Ma on prawo podjąć autonomiczną decyzję w zakresie tego, czy udostępni kopie danych, np. wydruk historii wypożyczeń, czy informację przetworzoną, w postaci wskazania zakresu przetwarzanych danych. Ma to istotne znaczenie dla kosztów realizacji żądań osób, których dane dotyczą. Dla przykładu wygenerowanie historii wypożyczeń z systemu bibliotecznego będzie prostą czynnością, ale przekazanie kopii wszelkiej korespondencji kierowanej do i od osoby, której dane dotyczą, a także dotyczącej tej osoby (np. pomiędzy pracownikami), może wymagać dużego nakładu czasu i pracy. W pierwszym wypadku ADO może zdecydować o udostępnieniu pełnej kopii danych osobowych, a w drugim o udostępnieniu informacji o zakresie przetwarzanych danych (tj. imię, nazwisko, treść wiadomości, data i godzina nadania wiadomości, nadawca, odbiorca, tytuł wiadomości). Przekazanie pierwszej kopii danych osobowych odbywa się bezpłatnie i jeżeli osoba, której dane dotyczą nie wskazała inaczej, następuje drogą elektroniczną z zachowaniem stosownych zabezpieczeń.

VI. Prawo do sprostowania danych (art. 16 RODO).

Jest to prawo do edycji lub poprawiania danych, dotyczy przede wszystkim sytuacji, w których w danych osobowych pojawił się błąd lub są przetwarzane niekompletnie. Administrator danych powinien dokonać aktualizacji niezwłocznie. Jest to szczególnie istotne, gdy błędnie wprowadzone dane mają wpływ na ograniczenie praw lub wolności osoby, której dane dotyczą, np. nieprawidłowo wprowadzony adres korespondencyjny uniemożliwi otrzymywanie informacji o zbliżającym się terminie zwrotu materiałów bibliotecznych. Przed sprostowaniem danych, niezbędne jest dokonanie weryfikacji tożsamości osoby, której dane dotyczą, zgodnie z wymaganiami art. 12 RODO.

VII. Prawo do usunięcia danych (art. 17 RODO).

Nazywane jest także prawem do bycia zapomnianym. Jest to jedno z najważniejszych uprawnień przysługujących osobie, której dane dotyczą, ponieważ w sposób bezpośredni przekłada się na zagwarantowanie jej odpowiedniego respektowania jej praw i wolności. Podkreślenia wymaga to, że nie w każdych okolicznościach dyrektor biblioteki będzie zobligowany do zrealizowania takiego żądania. Zgodnie z art. 17 ust. 3 RODO, nie będzie ono przysługiwało, w zakresie w jakim dane będą niezbędne:

1. do korzystania z prawa do wolności wypowiedzi i informacji,
2. do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy powszechnie obowiązujących przepisów prawa lub do wykonania zadania realizowanego w interesie publicznym,
3. z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3 RODO,
4. do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO, o ile prawdopodobne jest, że usunięcie danych, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania, lub
5. do ustalenia, dochodzenia lub obrony roszczeń.

Oznacza to, że w szczególności prawo do usunięcia danych nie będzie przysługiwało czytelnikowi, który nie zwrócił materiałów bibliotecznych, aż do momentu ich zwrotu lub wpłacenia ekwiwalentu za ich utratę. Podobnie, na przykład, jeżeli zleceniobiorca po zakończeniu współpracy zażąda usunięcia jego danych, spotka się z odmową, ponieważ przepisy o podatku od osób fizycznych oraz w zakresie ubezpieczenia społecznego, nakładają na bibliotekę obowiązek dalszego przetwarzania danych.

Prawo do bycia zapomnianym, zgodnie z art. 17 ust. 1 i 2 RODO przysługuje osobie, której dane dotyczą, jeżeli:

a. dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane,
b. osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania (np. adres e-mail lub nr telefonu czytelnika),
c. osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 RODO wobec przetwarzania,
d. dane osobowe były przetwarzane niezgodnie z prawem,
e. dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego, któremu podlega administrator,
f. dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego małoletnim, o których mowa w art. 8 ust. 1 RODO.

W przypadku danych upublicznionych na stronie internetowej biblioteki, np. zdjęć z wydarzeń udostępnionych w celach promocji, ADO także będzie miał obowiązek nie tylko usunąć dane, ale także powiadomić inne podmioty, którym udostępnił zdjęcia, o konieczności dokonania tych samych działań. Należy zwrócić uwagę na to, że dane usunięte ze strony biblioteki, które zostały upublicznione w celu promocji, w wielu przypadkach w dalszym ciągu będą mogły być przetwarzane w archiwum elektronicznym biblioteki, jako dokumentacja jej działalności. W takim wypadku należy osobę, której dane dotyczą poinformować o sposobie spełnienia ją żądania oraz w jakim zakresie, jakie dane i na jakiej podstawie, będą dalej przetwarzane. Należy także pamiętać, że usunięcie danych w formie papierowej, np. kart zobowiązań, formularzy konkursowych, danych zleceniobiorcy musi wiązać

się z usunięciem danych z systemów informatycznych i programów, w których te dane były przetwarzane. Dyrektor biblioteki powinien przechowywać wszystkie wnioski o usunięcie danych, wraz z odnotowaniem informacji o sposobie realizacji żądania. Jest to istotne ze względów dowodowych.

VIII. Prawo do ograniczenia przetwarzania (art. 18 RODO).

Ograniczenie przetwarzania jest szczególnym uprawnieniem osoby, której dane dotyczą, które realizuje się w jednym z czterech przypadków:

a. osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych,
b. przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
c. administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń (np. nagranie z monitoringu wizyjnego),
d. osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

Ograniczenie przetwarzania (lub zawieszenie przetwarzania) pozwala respektować prawa i wolności osoby, której dane dotyczą, w okresie, gdy administrator danych ustala, czy przysługuje jej realizacją żądania na mocy art. 15 lub 21 ust. 1 RODO. Jednocześnie daje osobie, której dane dotyczą możliwość decydowania o sposobie przetwarzania jej danych, w sytuacji, gdy powinny zostać usunięte. Może to dotyczyć na przykład żądania usunięcia zdjęć z kilku galerii na stronie biblioteki, gdzie na czas przeglądania zdjęć i podejmowania decyzji o usunięciu lub nie, zostaną wszystkie galerie ustawione, jako niewidoczne na stronie. Jeżeli przetwarzanie danych zostało ograniczone, dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego. O każdym ograniczeniu lub zakończeniu ograniczenia przetwarzania, należy poinformować osobę, której dane dotyczą.

IX. Prawo do przenoszenia danych (art. 20 RODO).

Osoba, której dane dotyczą ma prawo żądania otrzymania od administratora w powszechnie obowiązującym formacie elektronicznym jej danych osobowych w celu przekazania ich innemu administratorowi. Może żądać przekazania jej danych bezpośrednio lub aby zostały one przekazane innemu administratorowi. Prawo do przenoszenia danych ma szczególne znaczenie w dobie społeczeństwa informacyjnego, kiedy użytkownikom należy ułatwiać przenoszenie danych pomiędzy poszczególnymi usługodawcami. Prawo do przenoszenia danych dotyczy tylko tych danych, które są przetwarzane w systemach informatycznych, a podstawą przetwarzania jest zgoda tej osoby lub umowa z nią zawarta. Prawo do przenoszenia danych nie jest tożsame z żądaniem usunięcia danych, w szczególności gdy na bibliotece ciąży prawny obowiązek dalszego przechowywania danych. Warto zwrócić uwagę, że podstawą do przetwarzania danych osobowych czytelników są przepisy ustawy o bibliotekach, co oznacza, że co do zasady czytelnikowi nie przysługuje prawo do przenoszenia jego danych związanych z historią wypożyczeń.

X. Prawo do sprzeciwu na przetwarzanie danych (art. 21 RODO).

Prawo do wyrażenia sprzeciwu na przetwarzanie danych dotyczy przetwarzań realizowanych w bibliotece na podstawie prawnie uzasadnionego interesu biblioteki (art. 6 ust. 1 lit. f RODO) lub wykonywania zadania realizowanego w interesie publicznym. W bibliotece może to w szczególności dotyczyć przetwarzań realizowanych w związku z dokumentowaniem i promocją działalności biblioteki. W przypadku wniesienia sprzeciwu na takie przetwarzanie, należy dokonać testu wagi interesu osoby, której dane dotyczą w kontrze do prawnie uzasadnionych interesów biblioteki i w zależności od tego, który interes stoi powyżej drugiego, dyrektor biblioteki powinien podjąć decyzję o realizacji żądania sprzeciwu na przetwarzanie danych zgodnie z art. 21 ust. 1 RODO lub odmówić spełnienia żądania. W przypadku wykonywania żądania osoby, której dane dotyczą, należy zachować wniosek z żądaniem sprzeciwu oraz odnotować decyzję administratora. Czynności techniczne związane z oceną żądania, wagi praw i wolności osoby, której dane dotyczą oraz sposobu realizacji żądania może zrealizować IOD, w ramach swoich działań doradczych wobec administratora.

Dla przykładu, działania promocyjne bibliotek polegające na wysyłaniu korespondencji tradycyjnej z zaproszeniami na wydarzenia biblioteczne nie wymagają, w odróżnieniu od marketingu elektronicznego, uzyskania zgody osoby, której dane dotyczą. Jednakże ta osoba ma prawo w dowolnym momencie wnieść sprzeciw na otrzymywanie takich informacji (art. 21 ust. 2 RODO). W związku z tym należałoby w bibliotece prowadzić nie tylko listy odbiorców zaproszeń na wydarzenia, ale także listy osób, wykluczonych z ich otrzymywania. Przed każdą wysyłką pracownik merytoryczny odpowiedzialny za jej realizację, powinien dokonać weryfikacji listy odbiorców ze stworzoną listą osób wykluczonych z listy wysyłkowej.

XI. Prawo do niepodlegania zautomatyzowanym decyzjom, w tym profilowaniu (art. 22 RODO).

Co do zasady procesy biblioteczne nie powinny wiązać się z przetwarzaniem danych osobowych w sposób zautomatyzowany, w tym osoby, których dane dotyczą nie powinny podlegać profilowaniu, jednakże postęp nowych technologii otwiera takie możliwości. W szczególności nowoczesne systemy biblioteczne mogą na podstawie historii wypożyczeń czytelnika sugerować mu kolejne książki, które mogłyby go zainteresować. Jednak taki system może też mieć mniej korzystne dla czytelnika oblicze, na przykład mógłby na podstawie informacji o przedłużonych terminach wypożyczeń, zasugerować ograniczenie liczby materiałów, które będą udostępniane poza biblioteką. Jeżeli to system podejmuje decyzje, które mają wpływ na osobę, której dane dotyczą, musi mieć ona prawo do uprzedniego wyrażenia zgody na takie działanie. Dotyczy to także stron internetowych bibliotek, na których bardzo często zainstalowane są mechanizmy śledzące użytkowników, jak Pixel Facebooka, czy Google Analitics. Korzystanie z technologii, które śledzą i profilują użytkownika (a w tym wypadku także udostępniają jego dane do partnerów biznesowych oraz poza obszar UE) musi wiązać się z uzyskaniem uprzedniej (tutaj elektronicznej) zgody użytkownika. Warto podkreślić, że wynika to także z regulaminów tych usług, które nakładają na podmiot, korzystający z usługi nie tylko obowiązek pozyskania zgody, ale także udostępnienia każdemu użytkownikowi regulaminu tych usług, np. poprzez link w polityce prywatności. Korzystanie z tego typu usług powinno być umotywowane konkretnym celem działania, np. faktycznym dostosowywaniem treści strony i oferty bibliotecznej do podejmowanych przez użytkowników decyzji. Rolą IOD w bibliotece jest ocena adekwatności stosowania rozwiązań, które podejmują zautomatyzowane decyzje, w tym profilują dane, dla których administratorem danych jest biblioteka. W szczególności powinien on przeprowadzić ocenę skutków dla ochrony tych

danych, aby dokonać analizy, czy przetwarzanie faktycznie jest niezbędne, a także przygotować niezbędne informacje, które będą w przypadku wykorzystania tego typu technologii przekazywane w polityce informacyjnej.

4.2. Prawne podstawy przetwarzania danych osobowych. Czytelnicy, użytkownicy, uczestnicy wydarzeń, uczestnicy konkursów.

I. Czytelnicy.

Podstawę prawną przetwarzania danych czytelników i użytkowników biblioteki stanowi konieczność realizacji obowiązku prawnego wynikającego z ustawy o bibliotekach, ustawy o statystyce publicznej oraz ustawy o organizowaniu i prowadzeniu działalności kulturalnej, spełniony jest zatem warunek legalizujący przetwarzanie danych zgodnie z art. 6 ust. 1 lit. c RODO. Dane osobowe czytelników są przetwarzane w następujących celach:

- wykonywania zadań związanych z udostępnianiem i ochroną zbiorów bibliotecznych,
- statystycznych,
- zaspokajania potrzeb oświatowych, kulturalnych i informacyjnych ogółu społeczeństwa,
- upowszechniania wiedzy i kultury.

Konieczność ochrony materiałów bibliotecznych, wynikająca z przepisów ustawy o bibliotekach, wiąże się z koniecznością przetwarzania przez bibliotekę danych niezbędnych do ich odzyskania, w tym windykacji. W związku z tym pozyskuje się od czytelnika dane w zakresie imion, nazwisk, adresu korespondencyjnego, PESEL-u. Za zgodą czytelnika gromadzone są także nieobligatoryjne dane jak numer telefonu lub e-mail. W związku z koniecznością prowadzenia statystyk, czytelnik podaje także dane dodatkowe, wymagane udostępnianym co roku przez GUS formularzem K-03, jak na przykład kategoria społeczno-zawodowa.

II. Czytelnicy małoletni.

Podstawę prawną przy przetwarzaniu danych osobowych osób małoletnich, stanowią podobnie jak w przypadku czytelników i użytkowników pełnoletnich zapisy ustawy o bibliotekach, ustawy o statystyce publicznej oraz ustawy o organizowaniu i prowadzeniu działalności kulturalnej.

Rejestracja osób, które nie ukończyły 13 roku życia następuje poprzez złożenie pisemnego poręczenia jego rodzica lub opiekuna prawnego na zobowiązaniu. Małoletni jest wówczas uprawniony do korzystania zarówno z księgozbioru biblioteki jak również z usług oferowanych przez bibliotekę za okazaniem karty bibliotecznej, ale odpowiedzialność z tytułu niezwróconych materiałów ponosi opiekun ustawowy. Zgodnie z art. 15 i 20 Kodeksu cywilnego: „Ograniczoną zdolność do czynności prawnych mają małoletni, którzy ukończyli lat trzynaście (...). Osoba ograniczona w zdolności do czynności prawnych może bez zgody przedstawiciela ustawowego zawierać umowy należące do umów powszechnie zawieranych w drobnych bieżących sprawach życia codziennego". Co do zasady, zapisanie się do biblioteki oraz korzystanie z jej usług, można uznać za sprawę życia codziennego, i nie ma przeciwwskazań, by granica wiekowa osób, które same mogą zapisać się do biblioteki wynosiła 13 lat. Zapis do biblioteki nie będzie drobną sprawą życia codziennego, jeżeli biblioteka

przewiduje wysokie kary finansowe za niezwrócone materiały. W kodeksie cywilnym zostało jednoznacznie wskazane, że pełną zdolność do czynności prawnych nabywa się z chwilą uzyskania pełnoletności. Dlatego w sytuacji naliczania wysokich kar finansowych, mając na uwadze dochodzenie roszczeń od dłużnika np. za niezwrócone materiały, regulamin instytucji winien jasno określać granicę wiekową osoby, która sama może zapisać się do biblioteki tj. od 18 roku życia.

Jeżeli zapisu małoletniego do biblioteki dokonuje rodzic lub opiekun prawny, podpis dziecka na karcie zobowiązania nie będzie potrzebny. Osoby niepełnoletnie zapisywane są wówczas do biblioteki w obecności rodzica lub opiekuna prawnego, który składa pisemne oświadczenie o przyjęciu odpowiedzialności za zobowiązania niepełnoletniego w stosunku do biblioteki.

Warunki wyrażenia zgody na przetwarzanie danych osobowych przez dziecko w przypadku usług społeczeństwa informacyjnego zostały określone w art. 8 RODO w brzmieniu: „.zgodne z prawem jest przetwarzanie danych osobowych dziecka, które ukończyło 16 lat. Jeżeli dziecko nie ukończyło 16 lat, takie przetwarzanie jest zgodne z prawem wyłącznie i w przypadkach, gdy zgodę wyraziła lub zaaprobowała ją osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz w zakresie wyrażonej zgody". Ustawodawca unijny zaznacza, że państwa członkowskie mogą przewidzieć w swoim prawie niższą granicę wiekową, która musi wynosić co najmniej 13 lat. Projekt polskiej ustawy o ochronie danych osobowych zawierał zapisy, które obniżały ten wiek do lat 13, ale ostatecznie utrzymano granicę 16 lat. Zadaniem administratora jest natomiast podjęcie starań, uwzględniając dostępną technologię, by zweryfikować, czy osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem wyraziła zgodę na przetwarzanie danych. Takie potwierdzenie może nastąpić np. poprzez rozmowę telefoniczną lub wysłany e-mail. Powyższe zapisy należy przeanalizować przy korzystaniu z OPAC (On-line Public Access Catalog) katalogu powszechnego dostępu za pośrednictwem Internetu, który umożliwia przeszukiwanie w trybie on-line baz danych zawierających wydawnictwa dostępne w bibliotece, pozwala na zamawianie i rezerwowanie konkretnych pozycji oraz służy do samodzielnej obsługi konta czytelnika np. prolongaty wypożyczonych materiałów. W zależności od obowiązującego w bibliotece regulaminu dotyczącego zapisu czytelnika samo korzystanie z dodatkowej usługi proponowanej przez bibliotekę jakim jest zdalna rezerwacja i zamówienia pozycji wydawniczych, po uprzednim zebraniu wymaganych zgód przy zapisie w zależności od wieku czytelnika nie jest przeciwwskazaniem do posługiwania się tego typu narzędziem nawet przez osoby poniżej 13 roku życia oczywiście za zgodą i wiedzą rodzica lub opiekuna prawnego, który podając adres e-mail podczas zapisu otrzymuje jednorazowe hasło dostępu do w/w katalogu bibliotecznego. Warto zwrócić uwagę, że OPAC jest tylko częścią usługi bibliotecznej, która wymaga osobistej wizyty czytelnika w bibliotece, w celu założenia konta czytelnia, więc przepisy art. 8 RODO nie będą miały w tym zakresie zastosowania.

III. Uczestnicy konkursów.

Udział w konkursie, którego organizatorem jest biblioteka wymaga zaakceptowania regulaminu oraz wyrażenia zgody na przetwarzanie danych osobowych przez uczestnika (art. 6 ust. 1 lit. a RODO) lub ze względu na wiek uczestnika, jego opiekuna ustawowego. Zgodnie z motywem 32 RODO pozyskuje się jedną zgodę na wspólne (tożsame) cele przetwarzania, tzn. w związku z realizacją konkursu, wyłonieniem zwycięzców, wręczeniem nagród. Uczestnik powinien wyrazić zgodę, a także zaakceptować regulamin konkursu poprzez wypełnienie i podpisanie karty zgłoszeniowej lub zaznaczenie odpowiednich okienek w formularzu elektronicznym. Odrębną kwestię stanowi zgoda uczestnika na publikację wizerunku utrwalonego podczas konkursu/wydarzenia np. w mediach społecznościowych lub na stronie internetowej biblioteki. Taka zgoda powinna być nieobowiązkowa

i dodatkowa, a jej nie wyrażenie nie powinno wykluczać osoby z możliwości wzięcia udziału w konkursie/wydarzeniu.

W celu prawidłowego przeprowadzenia konkursu praktykuje się opracowanie regulaminu, regulującego kwestię zgłoszeń, przyznawania nagród, podatków, reklamacji, ale także obowiązku informacyjnego wobec uczestnika, który może być wypełniany kaskadowo, tzn. na częściowo na karcie zgłoszeniowej oraz w pełni w regulaminie.

Karty zgłoszeniowe uczestników konkursu należy przechowywać zgodnie z obowiązującą w bibliotece Instrukcja kancelaryjną, a zwycięzców przez 5 lat kalendarzowych po roku, w którym zakończył się konkurs zgodnie z wymaganiami przepisów podatkowych. Karty zgłoszeniowe zawierające zgody na wykorzystanie wizerunku należy przechowywać do momentu usunięcia tych danych lub wycofania zgody przez uczestnika.

Warto zwrócić uwagę, że w przypadku niektórych nagród, może być konieczne odprowadzenie podatku od wartości wygranej nagrody, z czym może wiązać się konieczność pozyskania dodatkowych danych osobowych na cele podatkowe. Biblioteka, która jest organizatorem konkursu, pełni funkcję płatnika w odniesieniu do wydawanych nagród. Zgodnie z art. 30 ust. 1 pkt 2 ustawy o podatku dochodowy podmiot przekazujący nagrodę jest zobowiązany pobrać zryczałtowany podatek dochodowy w wysokości 10% wartości nagrody. W oparciu o przepisy cyt. ustawy (art. 21 ust. 1 pkt 68), zwolnione z opodatkowania są:

- wygrane w konkursach i grach organizowanych i emitowanych (ogłaszanych) przez środki masowego przekazu (prasa, radio i telewizja, nie dotyczy to konkursów internetowych),
- konkursy z dziedziny nauki, kultury, sztuki, dziennikarstwa i sportu,
- nagrody związane ze sprzedażą premiową,
- wówczas, gdy jednorazowa wartość wygranych nagród nie przekroczy 2000,00 zł.

Zwolnione z obowiązku odprowadzania podatku są także nagrody o wartości nie przekraczającej 200,00 zł. Warto zwrócić uwagę, że ostatnie zwolnienie dotyczy sumy wartości nagród zdobytych przez jedną osobę w ciągu roku podatkowego. Należy podkreślić, że biblioteki zazwyczaj organizują konkursy promujące czytelnictwo, więc mogą powoływać się na jeden z warunków powyżej, o ile nagroda nie przekracza 2000,00 zł. Przy czym nie zwalnia to z obowiązku wykazania, że wskazana przesłanka faktycznie miała miejsce.

Na bibliotece jako organizatorze konkursu ciąży obowiązek obliczenia, pobrania i wpłaty do właściwego, dla osoby nagrodzonej, urzędu skarbowego zryczałtowanego podatku dochodowego od osób fizycznych. Osoba fizyczna, która otrzymała nagrodę musi uiścić 10% zryczałtowany podatek do wartości nagrody przed jej wydaniem. W świetle obowiązujących przepisów organizator konkursu nie ma obowiązku wystawić nagrodzonym osobom informacji podatkowej PIT-8C. Organizator składa jedynie roczną deklarację podatkowa PIT–8AR do właściwego Urzędu Skarbowego, wykazując ten podatek. Wspomniana deklaracja nie obejmuje żadnych danych osobowych osób nagrodzonych. Uczestnicy nie muszą też ujmować nagród w rocznych deklaracjach podatkowych PIT. Jedynie dla celów kontroli wskazane jest posiadanie przez organizatora konkursu numerów PESEL osób, które otrzymały nagrodę w celu ich identyfikacji. Pozyskany od zwycięzcy PESEL potwierdza, że nagroda została faktycznie wydana i że podatki zostały prawidłowo rozliczone.

Reasumując do przeprowadzenia konkursu administrator (organizator konkursu) zbiera od uczestników dane niezbędne do ich identyfikacji (imię, nazwisko, pseudonim), kontaktu z nimi (nr telefonu, adres e mail), a od zwycięzców, dane które są niezbędne do wręczenia nagrody (np. adres zamieszkania oraz może zbierać numer PESEL w celach podatkowych). Niewątpliwie dla ustalenia właściwego urzędu skarbowego płatnika (odbiorcy nagrody) koniecznym będzie podanie przez niego miejsca zamieszkania. Podanie danych jest wówczas konieczne do wypełnienia obowiązku prawnego wynikającego z przepisów podatkowych ciążącego na organizatorze konkursu.

IV. Uczestnicy wydarzeń.

Podstawą przetwarzania danych osobowych uczestników działań bibliotecznych jest umowa zawarta z uczestnikiem w momencie zaakceptowania przez niego regulaminu (np. szkolenia, zajęć), a w zakresie wizerunku przetwarzanego do celów promocyjnych, zgoda tego uczestnika. Organizator może zamieścić zgodę na nieodpłatne wykorzystanie wizerunku na karcie zapisu na zajęcia, przy czym zgoda nie powinna uzależniać możliwości udziału w zajęciach od jej wyrażenia. Ustawodawca unijny nie określa wprost, że zgoda musi zostać wyrażona w formie pisemnej, jednakże w celach dowodowych praktykowane jest, by wyrażenie zgody miało formę pisemną lub elektroniczną, poprzez zaznaczenie odpowiednich okienek w formularzu zapisu. Możliwym jest również wyrażenie pisemnej zgody wyłącznie na publikację wizerunku uczestników wydarzeń bez konieczności wypełnienia kart zapisu np. podczas spotkań autorskich, lekcji bibliotecznych. Zgodę na publikację wizerunku muszą wyrazić wówczas nie tylko uczestnicy wydarzeń ale również zaproszeni autorzy i pracownicy biblioteki prowadzący, np. lekcję biblioteczną. Jeżeli uczestnik zgłosi fakt wycofania zgody po zakończonym wydarzeniu, dane osobowe zostaną usunięte niezwłocznie bez konieczności przechowywania ich przez okres zgodny z obowiązującą w bibliotece instrukcją kancelaryjną. Dane osobowe w postaci wizerunku są publikowane przez bibliotekę (organizatora wydarzenia) od momentu zakończenia wydarzenia do czasu wycofania zgody. Wycofanie zgody w przedmiotowej kwestii jest równoznaczne z natychmiastowym usunięciem zdjęć z wizerunkiem ze strony internetowej instytucji, czy portalu społecznościowego. W kwestii publikacji wizerunku osób biorących udział w wydarzeniach bibliotecznych wyrażenie zgody na upublicznienie zdjęć z ich wizerunkiem jest niezbędne, chyba że zostały spełnione warunki przewidziane w przepisach Prawa autorskiego.

4.3. Obowiązek informacyjny.

Zgodnie z artykułami 13 i 14 RODO administrator powinien wypełnić obowiązek informacyjny wobec osób, od których dane są pobierane do przetwarzania. Obydwa powyższe artykuły precyzują dokładnie w jakich sytuacjach należy wypełnić obowiązek i jakie informacje należy przekazać.

Artykuł trzynasty określa obowiązek informacyjny, który należy spełnić wobec osób, od których dane są pozyskiwane bezpośrednio. By uczynić zadość przepisom należy przekazać osobom, których dane zamierza się przetwarzać następujące informacje:

- Określenie administratora, czyli Biblioteki, wraz z danymi kontaktowymi.
- Informację o sposobie kontaktu z Inspektorem Ochrony Danych.
- Określenie celu przetwarzania danych wraz z odniesieniem do konkretnej przesłanki legalizującej przetwarzanie, określonej w przepisach RODO oraz ewentualnie odwołanie do innych przepisów prawa (np. do Kodeksu Pracy).
- Oznaczenie odbiorców (zarówno znanych jak i prawdopodobnych), którym będą ujawnione dane, w tym tych przetwarzających dane poza Europejskim Obszarem Gospodarczym.
- Określenie okresu przetwarzania danych osobowych lub kryteria wyznaczenia takiego okresu.
- Wyszczególnienie jakie prawa ma osoba, której dane będą przetwarzane w ramach procesów bibliotecznych, czyli prawo do dostępu do danych, do ich sprostowania, do usunięcia, do przenoszenia, do ograniczenia przetwarzania oraz do wniesienia sprzeciwu wobec przetwarzania, a także prawo do odwołania zgody w dowolnym momencie, jeśli przetwarzanie odbywa się na podstawie wyrażonej zgody.
- Zawiadomienie o możliwości wniesienia skargi na sposób przetwarzania do Urzędu Ochrony Danych Osobowych.

- Informację o tym czy podanie danych jest dobrowolne czy konieczne, oraz o konsekwencjach odmowy podania danych.
- Informację o zautomatyzowanym przetwarzaniu danych, w tym o profilowaniu.

Artykuł czternasty z kolei precyzuje wypełnienie obowiązku informacyjnego wobec osób, których dane zostały pozyskane z innych źródeł niż podmiot danych. Dodatkowo należy poinformować osobę, której dane dotyczą o tym, z jakiego źródła pozyskała dane oraz o kategoriach odnośnych danych.

Wypełnienie obowiązku informacyjnego należy wykonać w różnych terminach w zależności sposobu pozyskania danych. W przypadku zbierania danych bezpośrednio klauzula musi być podana w momencie ich pozyskania. W przypadku pośredniego pozyskiwania danych należy wypełnić obowiązek informacyjny, w zależności od wykonywanych operacji w momencie pierwszej komunikacji, z osobą, której dane dotyczą, jednak nie później niż miesiąc od momentu otrzymania danych. Jeśli dane mają być ujawnione lub przekazane do innego odbiorcy, najpóźniej przy ich ujawnieniu. Obowiązek informacyjny musi być spełniony wobec wszystkich osób, których dane są przetwarzane przez każdego administratora, także gdy dane są udostępniane poszczególnym bibliotekom w ramach konsorcjum, za zgodą użytkownika.

Informacja powinna być przygotowana językiem jasnym, niezawiłym i zrozumiałym, tak by umożliwić każdej osobie, której dane dotyczą, jak najlepsze zrozumienie swoich praw oraz czynności, które będą podjęte w związku z przetwarzaniem.

Prawa osób, których dane dotyczą, powinny być każdorazowo selekcjonowane w odniesieniu do konkretnych przesłanek, na podstawie których odbywa się przetwarzanie, np. nie należy wpisywać do klauzuli informacyjnej prawa do wniesienia sprzeciwu, jeśli przetwarzanie będzie odbywać się na podstawie realizacji przepisu prawa. Prawo do wniesienia sprzeciwu jest możliwe do wykonania tylko wtedy, gdy dane są przetwarzane na podstawie przesłanek określonych w art. 6 lit. e i f RODO, czyli gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi lub gdy przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią. Dzięki dostosowaniu praw do konkretnych przesłanek można uniknąć ryzyka wprowadzenia w błąd osób, których dane są przetwarzane w bibliotece.

Osobę, której dane dotyczą, należy informować o wszelkich zmianach celów przetwarzania. Jeśli dyrektor biblioteki zamierzałby wykorzystać wcześniej pozyskane dane użytkowników do informowania o wydarzeniach organizowanych w jednostce, ma obowiązek, przed rozpoczęciem takiej czynności, poinformować wszystkich użytkowników o zmianie, a także prawie do wyrażenia sprzeciwu. Jeżeli informacje mają być przekazywane za pośrednictwem środków elektronicznych, jako newsletter, niezbędne jest także uprzednie zapytanie o zgodę na realizację takiego działania. Dobrą praktyką jest zamieszczenie klauzuli informacyjnej w regulaminie newslettera (obowiązek udostępnienia regulaminu usługi wynika z przepisów art. 8 UŚUDE).

Należy także zwrócić uwagę na obowiązki informacyjne związane z przetwarzaniem danych podczas ogólnodostępnych wydarzeń kulturalnych organizowanych w bibliotece. Dobrą praktyką jest przygotowanie regulaminu uczestnictwa w takich imprezach wraz z informacją o zasadach przetwarzania danych, w szczególności wizerunków uczestników wydarzenia, które będą upubliczniane w związku z promocją działalności biblioteki (Porównaj z podrozdział: 9.4. Wykorzystywanie wizerunków osób).

W pewnych przypadkach nie ma konieczności wykonywania obowiązku informacyjnego. Administrator, zgodnie z art. 13 ust. 4, jest zwolniony z jego wypełnienia w części lub w całości wtedy, gdy osoba, której dane dotyczą, otrzymała już informacje, które należy jej przekazać. W takim przypadku

należy przekazać tylko te informacje, które są nowością dla osoby, której dane dotyczą. Oczywiście po stronie administratora leży wykazanie, że niezbędne informacje faktycznie były osobie, której dane dotyczą znane, a obowiązek informacyjny wypełniony należycie. Jeżeli może to być trudne, zalecane jest wypełnienie pełnego obowiązku informacyjnego.

Obowiązek informacyjny może być spełniony na kilka sposobów. Jednostka może klauzulę informacyjną umieścić w regulaminie korzystania z zasobów biblioteki, który jest umieszczony na tablicy ogłoszeń, czy na stronie internetowej, można także każdorazowo dołączać informację do karty zobowiązań. Najlepszym wyjściem wydaje się każdorazowe udostępnianie przyszłemu czytelnikowi regulaminu podczas zapisu do biblioteki oraz dołączenie oświadczenia o zapoznaniu się z informacjami zawartymi w regulaminie do kart zobowiązań.

Osoby, których dane są przetwarzane w związku z działalnością kulturalną, warto poinformować o zasadach przetwarzania danych poprzez zamieszczenie w materiałach promocyjnych odnośników do klauzuli informacyjnej zamieszczonej w regulaminie udziału w wydarzeniach bibliotecznych. W takich przypadkach dobrze jest dołączać link do regulaminu we wszystkich materiałach publikowanych w Internecie, zaś do materiałów drukowanych dołączać kod QR, który umożliwi szybkie zapoznanie się zainteresowanych z niezbędnymi informacjami. Ponadto należy pamiętać, by treść regulaminu była także dostępna w formie papierowej w każdym oddziale bibliotek, tak by osoby, które rzadziej korzystają z zasobów cyfrowych, również mogły się z nią zapoznać.

4.4. Dobre praktyki, wytyczne i wskazówki.

GDY DANE POZYSKANO BEZPOŚREDNIO OD OSOBY, KTÓREJ DANE DOTYCZĄ [W TYM OD RODZICA LUB OPIEKUNA PRAWNEGO]

1. Administratorem Pani/a danych osobowych jest [**należy podać dane administratora, w tym dane kontaktowe]**
2. Administrator wyznaczył inspektora, z którym można się skontaktować w sprawach związanych z przetwarzaniem Pani/a danych **[należy podać dane kontaktowe]**
3. Pani/a dane osobowe będą przetwarzane w celu **[należy wskazać cel]**
4. Podstawą/ami przetwarzania Pani/a danych osobowych jest/są **[należy wskazać podstawę, jeżeli podstawą przetwarzania jest zgoda, należy poinformować o możliwości odwołania zgody w dowolnym momencie bez wpływu na przetwarzanie, które miało miejsce do momentu odwołania zgody]**
5. Odbiorcami Pani/a danych osobowych będą podmioty upoważnione do tego na podstawie przepisów prawa, a także **[należy wskazać innych odbiorców, np. biuro rachunkowe, firma IT świadcząca hosting, helpdesk, firma windykacyjna, kurierzy, operatorzy pocztowe, itp.]**
6. **[Jeżeli ten punkt nie ma zastosowania, należy go usunąć]** Pani/a dane mogą być/będą udostępnione do państwa trzeciego/organizacji międzynarodowej **[wskazać państwo trzecie, np. USA lub organizację międzynarodową, należy także poinformować o stwierdzeniu lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowied-**

nich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych]

7. Dane będą przechowywane przez **[wskazać okres, a gdy nie jest to możliwe, kryteria ustalania tego okresu]**
8. Ma Pan/i prawo żądania od administratora dostępu do swoich danych, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub wniesienia sprzeciwu wobec przetwarzania, a także do przenoszenia danych na podstawie i zgodnie z art. 15-22 RODO.
9. Ma Pan/i prawo wniesienia skargi na sposób przetwarzania przez administratora do Prezesa UODO (uodo.gov.pl)
10. Podanie danych jest **[dobrowolne / obowiązkiem wynikającym z .....]**, a nie podanie danych będzie skutkowało **[wskazać skutek, np. niemożliwością zawarcia umowy, zrezygnowaniem z usługi, itd.]**
11. **[Jeżeli ten punkt nie ma zastosowania, należy go usunąć]** Pani/a dane będą podlegały zautomatyzowanemu podejmowaniu decyzji na zasadach **[wskazać zasady]**. Wpływ i konsekwencje tego działania: **[wskazać]**
12. **[Jeżeli ten punkt nie ma zastosowania, należy go usunąć]** Pani/a dane będą podlegały profilowaniu na zasadach [wskazać zasady]. Wpływ i konsekwencje tego działania: **[wskazać]**

GDY DANE POZYSKANO Z INNEGO ŹRÓDŁA [NP. OD INNEGO ADMINISTRATORA LUB Z INTERNETU]

1. Administratorem Pani/a danych osobowych jest [**należy podać dane administratora, w tym dane kontaktowe]**
2. Administrator wyznaczył inspektora, z którym można się skontaktować w sprawach związanych z przetwarzaniem Pani/a danych **[należy podać dane kontaktowe]**
3. Pani/a dane zostały udostępnione przez **[...]** / zostały pobrane z ogólnodostępnych źródeł, jak strony internetowe, CeiDG, KRS, itp. **[wskazać możliwie precyzyjnie źródło danych]**
4. Administrator przetwarza Pani/a dane w zakresie **[wskazać, np. imienia, nazwiska, dane kontaktowe, adres, e-mail, itp.]**
5. Pani/a dane osobowe będą przetwarzane w celu **[należy wskazać cel, w sposób konkretny i zrozumiały dla odbiorcy]**
6. Podstawą/ami przetwarzania Pani/a danych osobowych jest/są **[należy wskazać podstawę, jeżeli podstawą przetwarzania jest zgoda, należy poinformować o możliwości odwołania zgody w dowolnym momencie bez wpływu na przetwarzanie, które miało miejsce do momentu odwołania zgody]**
7. Odbiorcami Pani/a danych osobowych będą podmioty upoważnione do tego na podstawie przepisów prawa, a także **[należy wskazać innych odbiorców, np. podmiot zapewniający wysyłanie newslettera, podmiot zapewniający poprawne działanie strony internetowej, agencja reklamowa wysyłająca newsletter, itp.]**
8. **[Jeżeli ten punkt nie ma zastosowania, należy go usunąć]** Pani/a dane mogą być/będą udostępnione do państwa trzeciego/organizacji międzynarodowej **[wskazać państwo trzecie, np. USA lub organizację międzynarodową, należy także poinformować o stwierdzeniu lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowied-**

nich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych]

9. Dane będą przechowywane przez **[wskazać okres, a gdy nie jest to możliwe, kryteria ustalania tego okresu]**
10. Ma Pan/i prawo żądania od administratora dostępu do swoich danych, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub wniesienia sprzeciwu wobec przetwarzania, a także do przenoszenia danych na podstawie i zgodnie z art. 15-22 RODO.
11. Ma Pan/i prawo wniesienia skargi na sposób przetwarzania przez administratora do Prezesa UODO (uodo.gov.pl)
12. Podanie danych jest **[dobrowolne / obowiązkiem wynikającym z .....]**, a nie podanie danych będzie skutkowało **[wskazać skutek, np. niemożliwością zawarcia umowy, zrezygnowaniem z usługi, itd.]**
13. **[Jeżeli ten punkt nie ma zastosowania, należy go usunąć]** Pani/a dane będą podlegały zautomatyzowanemu podejmowaniu decyzji na zasadach **[wskazać zasady]**. Wpływ i konsekwencje tego działania: **[wskazać]**
14. **[Jeżeli ten punkt nie ma zastosowania, należy go usunąć]** Pani/a dane będą podlegały profilowaniu na zasadach [wskazać zasady]. Wpływ i konsekwencje tego działania: **[wskazać]**

5 PRZEKAZYWANIE DANYCH OSOBOWYCH INNYM PODMIOTOM ORAZ PRZETWARZANIE DANYCH W IMIENIU BIBLIOTEKI

5.1. Powierzanie danych osobowych.

Jedną z najbardziej istotnych zmian wprowadzonych na mocy przepisów RODO była zmiana podejścia do przetwarzania danych osobowych w imieniu ADO. Specyficzny charakter tej zmiany polega w dużej mierze na tym, że od 25 maja 2018 r. każdy administrator musiał wprowadzić realne zmiany w tym obszarze. Kontrastowało to z wieloma obszarami, które pomimo rozpoczęcia bezwzględnego obowiązywania RODO nie wymagały nagłych zmian, ponieważ rozporządzenie było kontynuacją obowiązujących wcześniej uregulowań prawnych.

Żeby zrozumieć istotę powierzania danych osobowych, trzeba na początku uporządkować siatkę pojęciową związaną z takim działaniem. W języku potocznym, ale także w literaturze fachowej i wypowiedziach ekspertów funkcjonują następujące pojęcia:

- powierzanie danych osobowych,
- administrator,
- podmiot przetwarzający (zwany także procesorem).

W tekście RODO znajduje się wyłącznie określenie „administrator", które jak wskazano w podrozdziale 2.1. jest synonimem ADO lub „administratora danych" (wszystkie trzy pojęcia mają to samo znaczenie). Natomiast w tekście RODO nie znajduje się sformułowanie „powierzanie danych osobowych", które zostało w nim zastąpione sformułowaniem „przetwarzanie w imieniu administratora". Analogiczna sytuacja dotyczy słowa „procesor", które w tekście RODO występuje jako „podmiot przetwarzający". Do powierzenia danych osobowych dochodzi w sytuacji, w której ADO w dalszym ciągu pozostaje ich administratorem, a podmiot któremu przekazuje dane przetwarza je w jego imieniu (oznacza to, że nie decyduje o celach i sposobach przetwarzania przekazanych mu danych osobowych). ADO może też nie przekazywać danych tylko powierzyć procesorowi ich gromadzenie w swoim imieniu. Zakres powierzonych działań na danych osobowych jest szeroki i obejmuje m.in. wykorzystywanie, przechowywanie, poddawanie ochronie, interpretowanie, a nawet usuwanie. Do powierzenia danych osobowych dochodzi np. wtedy, kiedy firma zewnętrzna świadczy usługi BHP na rzecz biblioteki, bądź też podmiot zewnętrzny świadczy na jej rzecz usługi hostingu strony internetowej.

Powierzanie danych osobowych zostało szczegółowo uregulowane w przepisach RODO. Kluczowe znaczenie ma w tym przypadku art. 28 rozporządzenia, w którym zostały określone zasady podejmowania współpracy pomiędzy ADO a podmiotem przetwarzającym. Na początku warto podkreślić, iż zgodnie z przepisami RODO to na dyrekcji i pracownikach biblioteki ciąży obowiązek weryfikacji i wyboru odpowiedniego podmiotu przetwarzającego. W art. 28 ust. 1 RODO wskazano,

iż „jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą". W motywie 81. preambuły RODO doprecyzowano, że „chodzi o wiedzę fachową, wiarygodność i zasoby – wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom niniejszego rozporządzenia, w tym wymogom bezpieczeństwa przetwarzania". Oznacza to, że przed podpisaniem umowy powierzenia należy sprawdzić, czy podmiot który będzie przetwarzał dane osobowe w imieniu biblioteki jest do tego odpowiednio przygotowany, np. weryfikując czy posiada odpowiednie certyfikaty bezpieczeństwa, zaświadczenia o szkoleniach odbytych przez pracowników, wdrożone normy, polityki bezpieczeństwa i inne procedury potwierdzające potencjał w zakresie właściwej ochrony danych osobowych. Gwarancje można także wykazać poprzez stosowanie zatwierdzonego kodeksu postępowania.

Powierzenie danych osobowych musi odbywać się na podstawie umowy lub innego instrumentu prawnego. W przypadku bibliotek będzie to niemal zawsze pisemna umowa. Jej treść została określona w art. 28 ust. 3 RODO. Obowiązkowe elementy takiej umowy to:

- przedmiot i czas trwania przetwarzania,
- charakter i cel przetwarzania,
- rodzaj danych osobowych oraz kategorie osób, których dane dotyczą,
- obowiązki i prawa administratora.

W tym samym ustępie zostały precyzyjnie określone obowiązki podmiotu przetwarzającego. Umowa powinna stanowić w szczególności, że procesor:

- przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora,
- zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,
- podejmuje wszelkie środki bezpieczeństwa przetwarzania wymagane na mocy art. 32 RODO,
- przestrzega warunków korzystania z usług innego podmiotu przetwarzającego (podprocesora),
- biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w RODO,
- uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO (odnoszących się do bezpieczeństwa przetwarzania, zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu, zawiadamianie osób o naruszeniu ochrony ich danych osobowych, oceny skutków dla ochrony danych i uprzednich konsultacji)
- po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych,
- udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

Warto podkreślić, że „przetwarzanie danych osobowych wyłącznie na udokumentowane polecenie administratora" nie oznacza, że podmiot przetwarzający nie może wykonywać żadnych pojedyn-

czych czynności bez pisemnego potwierdzenia administratora. W tym przypadku kluczowe jest, aby sporządzić precyzyjną umowę pomiędzy ADO a procesorem i tam określić katalog czynności, jakie ma wykonywać podmiot przetwarzający. Jeżeli późniejsze działania będą mieściły się w ramach określonych w umowie to zgoda na każdą czynność nie jest potrzebna. Jeśli jednak podmiot przetwarzający uzna, że musi wykonać dodatkowe czynności, które nie zostały precyzyjnie wskazane w umowie, powinien uzyskać pisemną zgodę ADO, a przed jej uzyskaniem zaniechać takich działań.

W praktyce funkcjonowania bibliotek trudności sprawia kwestia podpowierzania danych osobowych. Takie działanie ma miejsce wtedy, gdy podmiot przetwarzający powierza dane osobowe otrzymane od biblioteki kolejnemu podmiotowi (np. swojemu podwykonawcy). Sytuację komplikuje to, że ten inny podmiot również może powierzyć dane kolejnym podmiotom, przez co oprócz procesorów można również wskazać podprocesorów. Warto podkreślić, że zgodnie z art. 28 ust. 2 RODO procesor nie może skorzystać z usług innego podmiotu w zakresie przetwarzania danych bez zgody administratora. Zgoda może mieć dwie formy. Pierwsza z nich to forma ogólna, na mocy której ADO wyraża zgodę na podpowierzanie danych osobowych innym podmiotom. Oczywiście o każdym podpowierzeniu ADO musi zostać niezwłocznie poinformowany, żeby zachować kontrolę nad tym, co dzieje się z danymi. Druga forma zgody jest szczegółowa i jest to rozwiązanie zapewniające większe bezpieczeństwo i kontrolę. Polega na tym, że ADO wyraża zgodę za każdym razem, kiedy podmiot przetwarzający chce powierzyć komuś dane. W obydwu przypadkach należy stworzyć takie warunki współpracy, żeby ADO miał możliwość dopełnić obowiązku informacyjnego wobec osób fizycznych, których dane dotyczą. Jednocześnie warto pamiętać, że zgodnie z art. 28 ust. 4 RODO podprocesor musi spełnić takie same wymagania bezpieczeństwa jak procesor, a jeśli dojdzie do zaniedbań to odpowiedzialność za podpowierzone dane spoczywa na procesorze.

5.2. Udostępnianie danych osobowych.

Udostępnianie danych osobowych jest czynnością dość często występującą w praktyce funkcjonowania bibliotek. Z udostępnianiem danych osobowych mamy do czynienia, gdy uprawniony podmiot zwróci się do ADO o przekazanie danych osobowych, posiadanych przez ADO, a ADO takie dane osobowe przekaże. Podmiotami najczęściej występującymi o udostępnienie danych osobowych są: Policja, prokuratura, sądy, komornik, ZUS, KRUS oraz bank.

Udostępnianie danych osobowych należy do czynności przetwarzania danych osobowych. Zgodnie bowiem z art. 4 pkt 2 RODO przetwarzanie oznacza „operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie". Zgodnie z powyższym udostępnianie danych osobowych należy do czynności ujawniania danych osobowych. Należy podkreślić, że w RODO nie znalazły się odrębne regulacje odnoszące się do udostępniania danych osobowych. Stąd też do udostępniania danych osobowych stosuje się przepisy RODO odnoszące się do przetwarzania danych osobowych.

ADO udostępnia dane osobowe wtedy, gdy istnieje podstawa prawna, która z jednej strony uprawnia podmiot występujący o udostępnienie danych do uzyskania danych, a z drugiej strony zobowiązuje ADO do przekazania danych. Podstawa prawna udostępnienia danych istnieje, gdy spełniona zostanie jedna z przesłanek określonych w art. 6 ust. 1 RODO (w przypadku udostępniania danych

osobowych zwykłych) lub też jedna z przesłanek określonych w art. 9 ust. 2 RODO (w przypadku udostępniania szczególnych kategorii danych osobowych).

Najczęściej udostępnienie danych osobowych ma miejsce w przypadku istnienia przepisu prawa krajowego stanowiącego podstawę prawną takiego działania.

Przykładowo:

- podstawę prawną udostępniania danych osobowych Policji stanowią przepisy ustawy o Policji oraz przepisy Kodeksu postępowania karnego,
- podstawę prawną udostępniania danych osobowych prokuraturze stanowią przepisy ustawy Prawo o prokuraturze,
- podstawę prawną udostępniania danych osobowych sądom stanowią w szczególności przepisy Kodeksu postępowania karnego oraz Kodeksu postępowania cywilnego,
- podstawę prawną udostępniania danych osobowych komornikowi stanowią przepisy ustawy o komornikach sądowych,
- podstawę prawną udostępniania danych osobowych ZUS stanowią przepisy ustawy o systemie ubezpieczeń społecznych.

Udostępnienie danych osobowych przez bibliotekę może nastąpić także między innymi w przypadku, gdy osoba, której dane dotyczą wyrazi zgodę na udostępnienie jej danych. Zgoda taka powinna spełniać warunki określone w art. 7 RODO.

Chociaż przepisy RODO nie określają formy złożenia wniosku o udostępnienie danych osobowych, przyjmuje się, że powinien być złożony w formie pisemnej lub w formie elektronicznej. Powinien być on także opatrzony podpisem osoby uprawnionej do wystąpienia z takim wnioskiem (w przypadku formy elektronicznej - kwalifikowanym podpisem elektronicznym lub profilem zaufanym). We wniosku powinna być wskazana także podstawa prawna udostępnienia danych osobowych, na którą powołuje się wnioskodawca. Przyjęcie takich rozwiązań zabezpieczy ADO przed sytuacjami udostępnienia danych podmiotom nieuprawnionym.

Udostępnienie może nastąpić, w zależności od woli wnioskodawcy, w formie pisemnej lub też w formie elektronicznej. Jednakże w przypadku przekazywania danych osobowych w formie elektronicznej ADO powinien zabezpieczyć dane osobowe przed dostępem nieuprawnionych podmiotów (np. poprzez zastosowanie szyfrowania).

Wyjątkowo, w szczególnych sytuacjach, dopuszczalne jest udostępnienie danych osobowych telefonicznie, ale w takim przypadku ADO musi mieć pewność co do tożsamości osoby, której udostępnia dane osobowe. W przypadku udostępnienia danych osobowych w ten sposób zaleca się sporządzenie notatki służbowej dokumentującej tę czynność.

Oceny zasadności wniosku o udostępnienie danych osobowych dokonuje i decyzję o udostępnieniu danych osobowych podejmuje ADO. Podejmując decyzję w tej sprawie ADO musi ustalić istnienie podstawy prawnej udostępnienia danych osobowych, z uwzględnieniem opinii IOD. W przypadku braku podstawy prawnej udostępnienia danych osobowych ADO odmawia udostępnienia. Odmowa powinna być dokonana w takiej samej formie jak wniosek o udostępnienie.

Chociaż RODO nie przewiduje takiego obowiązku, w bibliotece powinien być prowadzony rejestr (ewidencja) udostępnień danych osobowych zawierający informacje dotyczące poszczególnych udostępnień. Powinny w nim być uwzględnione:

- dane podmiotu, któremu udostępnione zostały dane osobowe,
- dane osoby lub osób, których dane zostały udostępnione na podstawie wniosku,
- rodzaj i zakres udostępnionych danych osobowych,
- podstawa prawna udostępnienia danych osobowych,
- sposób udostępnienia danych osobowych,
- data udostępnienia danych osobowych.

Warto przypomnieć, że z chwilą udostępnienia danych osobowych podmiot, któremu dane zostały udostępnione staje się ich administratorem. Podmiot ten ustala bowiem cele i sposoby przetwarzania przekazanych mu danych. W związku z tym ciążą na nim wszelkie obowiązki związane z ochroną przekazanych mu danych osobowych.

5.3. Współadministrowanie.

Poprzez przepisy RODO dano także możliwość współadministrowania danymi osobowymi przez dwóch lub większą liczbę ADO. Do współadministrowania dochodzi wówczas, gdy więcej niż jeden podmiot ustala cele i sposoby przetwarzania danych. W takich przypadkach wszystkie podmioty, które zamierzają współadministrować danymi wspólnie, muszą wyznaczyć, jakie zamierzają osiągnąć przetwarzaniem cele oraz określić sposoby wspólnego przetwarzania danych. W przepisach RODO szczególny nacisk położono na realizację praw osób, których dane dotyczą. Tak jest także w przypadku współadministrowania. W związku z powyższym administratorzy, którzy zamierzają współadministrować danymi muszą w przejrzysty i jasny sposób określić swoją odpowiedzialność w zakresie wykonywania praw osób, których dane będą przetwarzać oraz podać informacje, do których są zobowiązani poprzez art. 13 i 14 RODO. Ustalenia współadministratorów dotyczące wykonania przetwarzania danych (realizacja praw osób, których dane dotyczą, określenie relacji pomiędzy poszczególnymi administratorami, określenie zakresów obowiązków współadministratorów) powinny być jawne dla osób, których dane dotyczą.

Przykładem współadministrowania może być organizowanie przez bibliotekę wydarzenia lub konkursu wspólnie z innym podmiotem (np. z inną instytucją kultury, jednostką samorządu terytorialnego lub sponsorem zewnętrznym). Należy wtedy wspólnie określić jakie są cele przetwarzania oraz to, który ze współadministratorów będzie odpowiadał za wykonanie poszczególnych obowiązków związanych z realizacją praw uczestników wydarzenia/konkursu.

Współadministrowaniem nie będą natomiast wszelkiego rodzaju usługi, które są realizowane dla biblioteki przez podmioty zewnętrzne, takie jak np. świadczenie wsparcia informatycznego lub wykorzystywanie zewnętrznego, elektronicznego systemu obsługi czytelników. W przypadku realizacji usług należy każdorazowo zawierać umowy powierzenia przetwarzania danych osobowych, gdyż usługodawcy nie realizują wtedy swoich celów przetwarzania, a jedynie cele biblioteki, która im te dane powierzyła do przetwarzania, by zrealizować swoje zadania, nie mając do realizacji tych zadań swoich własnych zasobów.

6 DOKUMENTACJA OCHRONY DANYCH OSOBOWYCH

6.1. Wykorzystanie istniejącej w bibliotece dokumentacji ochrony danych.

Przed rozpoczęciem bezwzględnego obowiązywania RODO administratorzy danych opierali sformalizowane procedury ochrony danych osobowych na rozporządzeniu w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. W przepisach tego rozporządzenia określono szczegółowo jak powinna wyglądać dokumentacja bezpieczeństwa danych. Ten akt prawny został uchylony, ale nadal może być punktem wyjścia do stworzenia właściwej dokumentacji ochrony danych osobowych. W szczególności nie należy rezygnować automatycznie z już funkcjonujących w bibliotece dokumentów.

Zgodnie z uchylonym aktem prawnym na dokumentację bezpieczeństwa danych składa się polityka bezpieczeństwa oraz instrukcja zarządzania systemami informatycznymi. Są to dokumenty, które przed wejściem w życie przepisów RODO, powinny być w każdej bibliotece, a zatem stanowią doskonały punkt wyjścia do stworzenia polityk i procedur zgody z RODO. Warto także podkreślić, że ADO tworząc i aktualizując dokumentację ochrony danych korzysta ze wsparcia IOD, którego obowiązkiem jest także monitorowanie zgodności z przepisami oraz aktualności dokumentacji oraz zgłaszanie wszelkich koniecznych zmian do ADO.

I. Polityka bezpieczeństwa.

Polityka bezpieczeństwa jest dokumentem, który w dniu wejścia w życie przepisów RODO określał precyzyjnie jakie dane, w jakich obszarach i w jaki sposób mogą być przetwarzane w bibliotece. Polityka bezpieczeństwa to zbiór dokumentów, w skład których na mocy uchylonego rozporządzenia MSWiA wchodziły w szczególności:

- wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe,
- wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
- opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,
- sposób przepływu danych pomiędzy poszczególnymi systemami,
- określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

W przepisach RODO nie podano tak szczegółowych instrukcji co do wyglądu dokumentów jak w przypadku wspomnianego aktu prawnego. Wspomniany wykaz zbiorów z podziałem na programy z informacją o polach informacyjnych wraz z określeniem ogólnych środków technicznych i organizacyjnych dla zapewnienia bezpieczeństwa można uznać za doskonały punkt wyjścia do rejestru czynności przetwarzania. Zasadne jest pozostawienie informacji o obszarach przetwarzania danych osobowych – jest to niezbędne do zapewnienia rozliczalności danych. Z pewnością określone w dokumentacji środki techniczne oraz organizacyjne będą wymagały uwzględnienia wymagań art. 5, 24 oraz 32 RODO. Dodatkowo w polityce często były określone procedury nadawania upoważnień do przetwarzania danych, obligowania do zachowania poufności, zasady niszczenia danych, które po wejściu przepisów RODO, pozostają niezbędne i aktualne.

II. Instrukcja Zarządzania Systemami Informatycznymi.

Instrukcja Zarządzania Systemami Informatycznymi [IZSI] stanowi zbiór zasad i procedur przetwarzania danych w ramach systemów informatycznych. W szczególności określa zakres odpowiedzialności poszczególnych osób odpowiedzialnych za ochronę danych, uprawnienia i zobowiązania użytkowników, zasady przyznawania i kontroli dostępów do systemów informatycznych, a także procedury zapewniania ochrony danych przetwarzanych w formie elektronicznej.

IZSI zgodnie z uchylonym rozporządzeniem powinna była zawierać co najmniej:

- procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności,
- stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem,
- procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu,
- procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania,
- sposób, miejsce i okres przechowywania:
- elektronicznych nośników informacji zawierających dane osobowe,
- kopii zapasowych.
- sposób zabezpieczenia systemu informatycznego przed działalnością złośliwego oprogramowania,
- procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Zgodnie z przepisami RODO taki dokument nie jest wprost wymagany, jednakże konieczność dostosowania środków ochrony do ryzyk związanych z przetwarzaniem danych, powinna oznaczać, że jeżeli ADO przetwarza dane w systemach informatycznych, to wdrożenie odpowiedniej IZSI jest niezbędne. Pozostawienie i zaktualizowanie dotychczas obowiązującej instrukcji, a także dalsze jej aktualizowanie, konieczne ze względu na szybko postępującą technologię i zagrożenia cyberbezpieczeństwa, pozwoli ADO zachować większą kontrolę nad systemami informatycznymi. Sumiennie wykonany dokument będzie bowiem stanowił organizacyjny środek ochrony dla zasobów chronionych przetwarzanych w systemach informatycznych, ale również przyczyni się do ochrony interesu administratora danych. Instrukcja określa między innymi jakie kto może mieć uprawnienia, w jakich sytuacjach i na jakich zasadach nadawane są loginy i hasła do systemów informatycznych, w jaki sposób oraz jak często tworzone są kopie zapasowe oraz kto i w jaki sposób dokonuje przeglądu nadzorowanych systemów.

Pierwszym krokiem do prowadzenia dokumentacji ochrony danych zgodnej z RODO jest inwentaryzacja procedur już funkcjonujących w bibliotece. Częstym błędem kadry kierowniczej bibliotek lub pracujących w nich IOD jest odcięcie się od tego co było i tworzenie wszystkich polityk i procedur na nowo. Warto podkreślić, iż wiele dokumentów można po niewielkich poprawkach używać dalej. Wśród dokumentów zapewne znajdą się i takie, które można użyć ponownie bez zmian.

Szeroki zakres zadań pracowników bibliotek oraz rotacja w zatrudnieniu powodują, że często administratorzy oraz osoby pracujące w instytucji nie mają wystarczającej wiedzy o istniejącej dokumentacji. Prawidłowo sporządzona i odpowiednio wdrożona dokumentacja ochrony danych osobowych, na którą przede wszystkim składa się polityka bezpieczeństwa oraz instrukcja zarządzania systemami informatycznymi to sprawdzony sposób na skuteczną ochronę zasobów chronionych, a szkolenia pracowników z zasad zawartych w dokumentach powinno być jednym z ważniejszych zadań realizowanych regularnie przez IOD.

6.2. Dokumenty które muszą znajdować się w bibliotece zgodnie z RODO.

Dokumenty, które powinny znajdować się w każdej bibliotece można podzielić na trzy grupy, tzn. wymagane wprost na mocy RODO, wymagane pośrednio na mocy RODO (czyli stanowiące dobrą praktykę), a także obowiązujące przez RODO, które ADO postanowił zachować po niezbędnej aktualizacji.

I. Dokumenty wymagane wprost na mocy RODO.

- Rejestr czynności przetwarzania – art. 30 RODO, rejestr ten został szczegółowo omówiony w podrozdziale 6.3.
- Rejestr kategorii czynności przetwarzania – art. 30 RODO, rejestr ten został szczegółowo omówiony w podrozdziale 6.4.
- Ocena skutków dla ochrony Danych – art. 35 RODO, zagadnienie zostało szczegółowo omówione w podrozdziale 8.3.
- Procedura postępowania w przypadku naruszenia ochrony danych – art. 33 RODO, przez dokumenty związane z naruszeniem należy rozumieć: procedurę postępowania w przypadku naruszenia, procedurę w przypadku zawiadomienia osób których dane dotyczą o naruszeniu, wzór zawiadomienia o naruszeniu, zgłoszenie naruszenia do UODO oraz rejestr naruszeń. Dokładne omówienie znajduje się w rozdziale 11.4 i 11.5.
- Procedura powierzenia danych – art. 28 RODO, przez dokumenty związane z powierzeniem danych należy rozumieć: procedurę postępowania w przypadku powierzenia danych (m.in. informację kiedy dochodzi do powierzenia danych, wskazanie osób odpowiedzialnych). W swoich dokumentach ADO powinien mieć wzór umowy powierzenia. Dokładne omówienie tego zagadnienia znajduje się w podrozdziale 5.1.

II. Dokumenty, które są pośrednio wymagane na mocy RODO, stanowiące dobrą praktykę.

- Wzór zawiadomienia Prezesa UODO o wyznaczeniu, zmianie oraz odwołaniu IOD – o obowiązku wyznaczenia Inspektora Ochrony Danych mowa jest w art. 37 RODO. Dodatkowo

w artykule 10. Ustawy ODO mowa jest o zawiadomieniu Prezesa UODO o wyznaczeniu, zmianie oraz odwołaniu IOD. Na stronie internetowej UODO można znaleźć gotową procedurę oraz odpowiednie formularze.

- Procedura nadawania, zmiany oraz odwołania upoważnień do przetwarzania danych osobowych oraz ich ewidencja – obowiązek posiadania upoważnień do przetwarzania danych osobowych wynika z kilku przepisów RODO (m.in. art. 5, art. 24, art. 32). We wskazanych artykułach nie zostało wprost wskazane, iż ADO powinien posiadać procedurę nadawania/zmiany/odwołania upoważnień, brak też wprost informacji o wymogu prowadzeniu ewidencji upoważnień. W związku z tym niektórzy mogą uważać, że takie dokumenty mają charakter fakultatywny. Warto jednak podkreślić, że ich posiadanie usystematyzuje pracę zarówno pracowników (szybka i przejrzysta rozliczalność, poprzez wiedzę o zakresie uprawnień), jak i kadry kierowniczej (każda osoba będzie wiedziała w jaki sposób nadać/zmienić/odwołać określone upoważnienia). Procedury nadawania /zmiany/odwołania upoważnień nie muszą być obszerne, jednak ważne jest aby miały pokrycie w rzeczywistości.
- Wzór obowiązku informacyjnego – obowiązek informacyjny został usankcjonowany w art. 13. i 14. RODO. Dobrą praktyką ADO jest posiadanie w swojej dokumentacji wzorów obowiązków informacyjnych dla określonych procesów. W bibliotece mogą to być obowiązki informacyjne m.in. kierowane do pracowników, czytelników, uczestników konkursów, uczestników szkoleń oraz odbiorców newslettera.
- Wzór zgody – konieczność pozyskiwania potwierdzenia wyrażenia zgody na przetwarzanie danych osobowych wskazano w art. 7 RODO. Dobrą praktyką jest posiadanie stałego formularza zgody, aby móc w prosty i efektywny sposób ją pozyskać.
- Procedura udostępniania danych – w dokumentacji powinna być procedura udostępnienia danych oraz wzór wniosku, aby w sytuacji wpłynięcia zapytania każdy pracownik wiedział co należy zrobić, a także kto formalnie jest uprawniony do oceny wniosków oraz udostępniania danych.
- Wzór oświadczenia o poufności – oświadczenie o poufności powinien podpisać zarówno pracownik, który będzie miał dostęp do danych (jeżeli taka formuła nie znajduje się np. w upoważnieniu), jak i pracownik/współpracownik nieprzetwarzający bezpośrednio danych osobowych, np. personel sprzątający, serwisant sprzętu.
- Dokumenty związane z monitoringiem zgodności przetwarzania danych osobowych – wśród tych dokumentów powinna znajdować się procedura przeprowadzania sprawdzeń – kiedy i kto wykonuje sprawdzenia, procedura przeprowadzenia sprawdzenia planowego i doraźnego oraz wzór sprawozdania ze sprawdzenia
- Analiza ryzyka – przeprowadzenie analizy ryzyka jest obowiązkiem ADO wynikającym z RODO. Wśród dokumentów które warto posiadać znajduje się procedura analizy ryzyka, w której wskazana jest metodyka jej przeprowadzania.
- Procedura realizacji praw osoby, której dane dotyczą – do prawa osób, których dane dotyczą odniesiono się w art. 15-22 RODO. W dokumentacji u administratora danych powinny znaleźć się procedury umożliwiające realizację przysługujących praw.

III. Dokumenty i procedury znajdujące się już u ADO.

Jak wskazano wcześniej, część procedur funkcjonujących w bibliotece na mocy już nieobowiązujących przepisów, bądź też aktów prawnych niezwiązanych z ochroną danych osobowych może w dalszym ciągu funkcjonować w instytucji. Wśród nich warto wskazać:

- Politykę bezpieczeństwa (danych osobowych),
- Instrukcję Zarządzania Systemami Informatycznymi,
- Regulamin korzystania z biblioteki,
- Regulamin korzystania z czytelni,
- Regulamin konkursu,
- Regulamin newslettera,
- Regulamin wydarzeń/imprez,
- Regulamin pracy,
- Regulamin Zakładowego Funduszy Świadczeń Socjalnych,
- Regulamin Kasy Zapomogowo Pożyczkowej,
- Regulamin rekrutacji,
- Instrukcję przeciwpożarową,
- Instrukcję BHP.

Pomimo, że nie są to dokumenty wprost kojarzące się z zasadami przetwarzania danych, to mają wpływ na to działanie, w szczególności ochronę danych, określają sposób zbierania danych, zakres przetwarzanych danych, cele i sposoby przetwarzania. W większości regulaminów będzie także realizowany obowiązek informacyjny z art. 13 ust. 1 i 2 RODO.

6.3. Rejestr czynności przetwarzania danych osobowych.

Rejestr czynności przetwarzania jest istotnym narzędziem służącym do zapewnienia nadzoru nad przetwarzanymi danymi osobowymi. Zakres informacyjny rejestru pozwala ADO określić jakie dane są w jakich celach, na jakiej podstawie i w jakim zakresie przetwarzane, a także komu są ujawniane i jak długo powinny być przechowywane. Jest to narzędzie, które umożliwia prowadzenie retencji danych. Rejestr stanowi także punkt wyjścia do nadawania upoważnień do przetwarzania danych osobowych. Dobrze prowadzony i na bieżąco aktualizowany rejestr, pozwala ADO zapewnić rozliczalność danych (art. 5 RODO). Obowiązkiem IOD będzie monitorowanie zgodności rejestru ze stanem faktycznym, a także informowanie ADO o konieczności jego aktualizacji. Rejestr czynności przetwarzania biblioteki z wyłączeniem kolumny dotyczącej zastosowanych środków ochrony danych, należy uznać za informację publiczną. Nie ma obowiązku publikowania rejestru na stronie internetowej biblioteki, jednak nie ma podstaw do odmowy jego udostępnienia, z ograniczeniem informacji, które mogłyby wpłynąć na osłabienie systemu ochrony danych w bibliotece.

Rejestr czynności przetwarzania zgodnie z art. 30 ust. 5 RODO powinien prowadzić każdy administrator, który:

- Zatrudnia powyżej 250 osób,
- Przetwarza dane osobowe w sposób systematyczny (brak charakteru sporadycznego),
- Przetwarza szczególną kategorię danych osobowych (art. 9 ust. 1 RODO),
- Przetwarza dane osobowe dotyczące wyroków skazujących i naruszeń prawa (art. 10 RODO).

Przesłanką do prowadzenia przez biblioteki rejestru czynności przetwarzania jest brak sporadycznego charakteru przetwarzania danych osobowych. Rejestr czynności przetwarzania prowadzony jest w formie pisemnej, w tym w formie elektronicznej. Tworzenie rejestru należy zacząć od inwentaryzacji zasobów chronionych u administratora poprzez wyodrębnienie czynności przetwarzania.

Podążając za informacjami zawartymi w książce pt. „Wykonywanie obowiązków ABI, przyszłego inspektora ochrony danych, w świetle ogólnego rozporządzenia o ochronie danych", której wydawcą

było Biuro Generalnego Inspektora Ochrony Danych Osobowych w 2016 r., rejestr czynności przetwarzania należy rozumieć jako wykaz przetwarzanych zbiorów danych, na które dzieli się wszystkie przetwarzane u danego administratora danych informacje ze względu na zakres przetwarzanych danych, cele przetwarzania oraz kategorie odbiorców, którym dane zostają udostępnione. Natomiast w poradniku opublikowanym przez UODO pt. „Wskazówki i wyjaśnienia dotyczące rejestrowania czynności i kategorii czynności przetwarzania określonego w art. 30 ust. 1 i 2 RODO" mowa jest o czynnościach przetwarzania jako o zespole powiązanych ze sobą operacji na danych, wykonywanych przez jedną lub kilka osób, które można określić w sposób zbiorczy, w związku z celem, w jakim te czynności są podejmowane.

W obydwu opracowaniach wskazano, w jaki sposób należy rozumieć czynność przetwarzania. W poniższej tabeli przedstawiono najczęściej występujące w bibliotece zbiory danych i odpowiadające im czynności przetwarzania danych.

Tabela 1. Przykładowe zbiory danych i operacje na danych w bibliotece.

NAZWA ZBIORU DANYCH	ODPOWIADAJĄCE ZBIOROM CZYNNOŚCI PRZETWARZANIA
Pracownicy	Czynności związane z zatrudnieniem na umowę o pracę
Umowy cywilno-prawne	Czynności związane ze współpracą na umowę cywilno-prawną
Współpracownicy	Czynności związane z realizacją usług na podstawie umów o współpracę
Kontrahenci	Czynności związane z realizowaniem umów i rozliczaniem faktur
Zakładowy Fundusz Świadczeń Socjalnych	Czynności związane z przyznawaniem świadczeń z Funduszu
Praktykanci	Czynności związane z realizacją zadań w ramach praktyk
Stażyści	Czynności związane z realizacją zadań w ramach stażu
Wolontariusze	Czynności związane z realizacją zadań w ramach wolontariatu
Konkursy	Czynności związane z realizacją konkursów
Imprezy/wydarzenia	Czynności związane z organizowaniem imprez / wydarzeń
Kandydaci do pracy	Czynności związane z rekrutacją pracowników
Czytelnicy	Czynności związane z korzystaniem przez czytelników z zasobów biblioteki
Szkolenia	Czynności związane z organizowaniem i prowadzeniem szkoleń
Newsletter	Czynności związane z realizacją wysyłki newslettera
Darczyńcy i sponsorzy	Czynności związane z przyjmowaniem oraz rozliczaniem darów i datków
Przetargi	Czynności związane z realizacją przetargów
Rejestr poczty wychodzącej / przychodzącej	Czynności związane z rejestrowaniem korespondencji
Kontakty	Czynności związane z kontaktem z administratorem

Źródło: Opracowanie własne.

Zgodnie z art. 30 ust. 1 RODO rejestr czynności przetwarzania powinien zawierać:

- pełną nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów (w odniesieniu do czynności, które podlegają współadministrowaniu),
- imię, nazwisko oraz dane kontaktowe inspektora ochrony danych,
- cele przetwarzania – np. realizacja zadań w ramach umowy o współpracę,
- opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych – opis osób, których dane dotyczą w ramach określonej czynności przetwarzania oraz określenie czy są to dane zwykłe czy szczególna kategoria danych, np. osoby realizujące zadana zatrudnione na podstawie umowy o pracę oraz osoby których dane zostały podane do kontaktu, ZUS; szczególna kategoria danych oraz dane zwykłe,
- kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych – należy wymienić wszystkich odbiorców danych osobowych. Zgodnie z definicją zawartą w art. 4 RODO odbiorca oznacza „osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców". W praktyce w punkcie tym warto umieścić wszystkie podmioty, którym dane zostaną ujawnione, np. bank, biuro rachunkowe, firmę kurierską, Urząd Skarbowy, Zakład Ubezpieczeń Społecznych,
- gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwę tego państwa lub organizacji międzynarodowej,
- jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych – jak długo będą przetwarzana dane osobowe. W niektórych przypadkach jest to określone wprost w aktach prawnych, w pozostałych przypadkach okres przechowywania danych osobowych określa ADO.
- jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa – należy krótko określić zastosowane środki bezpieczeństwa np. zastosowano okresową zmianę hasła, do niszczenia dokumentów wykorzystywane są niszczarki. Można również odnieść się do konkretnej polityki obowiązującej w bibliotece.

Rejestr powinien podlegać okresowym przeglądom realizowanym przez IOD. Natomiast za treść, tzn. zawartość rejestru odpowiada ADO. Ważne jest, aby czynności przetwarzania były identyfikowane oraz aktualizowane we współpracy z osobami przetwarzającymi dane w bibliotece. To pozwoli zapewnić kontrolę nad tym, że pewne procesy przetwarzania ustały lub mają mieć miejsce. Dodatkowo osoby odpowiedzialne za poszczególne czynności merytoryczne będą w stanie zweryfikować zakres danych przetwarzanych w ramach danej czynności, podstawy prawne, cele przetwarzania oraz podmioty, którym te dane są ujawniane. Dobrze opracowany rejestr stanowi doskonały punkt wyjścia do opracowania poprawnych klauzul informacyjnych. Należy zwrócić uwagę, aby odbiorcy danych wskazani w rejestrze oraz klauzuli informacyjnej byli zgodni.

Przykładowy wzór rejestru czynności przetwarzania znajduje się w rozdziale 6.6 – tabela 1 i 2.

6.4. Rejestr kategorii czynności przetwarzania danych osobowych.

Rejestr kategorii czynności przetwarzania służy zapewnieniu skutecznego nadzoru nad danymi, które są powierzane bibliotece w celu ich przetwarzania w imieniu innego administratora. Zgodnie z art. 30 ust. 2 RODO rejestr kategorii czynności przetwarzania prowadzi każdy administrator, któ-

remu powierzono dane. Rejestr ten można określić jako „specyficzny spis umów powierzenia". Jest on prowadzony w formie pisemnej, w tym w formie elektronicznej (np. arkusz kalkulacyjny). Zgodnie z RODO rejestr kategorii czynności przetwarzania powinien zawierać:

- pełną nazwę i dane kontaktowe podmiotu przetwarzającego, tzn. biblioteki której powierzono dane do przetwarzania,
- imię i nazwisko dane kontaktowe IOD,
- nazwę i dane kontaktowe każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora,
- kategorie przetwarzań dokonywanych w imieniu każdego z administratorów – należy określić je zgodnie z zapisami zawartej umowy powierzenia danych,
- gdy ma to zastosowanie – przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej,
- jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa – należy krótko określić zastosowane środki bezpieczeństwa np. zastosowano okresową zmianę hasła, do niszczenia dokumentów wykorzystywane są niszczarki. Można również odnieść się do konkretnej polityki obowiązującej w bibliotece.

W praktyce, aby rejestr mógł być skutecznym wsparciem dla ADO dodaje się nieobowiązkowe kolumny:

- data zawarcia umowy,
- data zakończenia umowy,
- sposób postępowania z danymi po zakończeniu umowy,
- informacje o dalszym powierzeniu danych,
- specyficzne zapisy z umowy, np. niestandardowe środki ochrony danych.

Należy podkreślić, że w przypadku bibliotek, bardzo rzadko będzie dochodzić do przetwarzania danych w imieniu innego administratora. Takie działanie może być realizowane przez biblioteki wojewódzkie w ramach konsorcjów bibliotek, gdzie biblioteka wojewódzka zapewnia centralny serwer danych obsługujący system biblioteczny, z którego korzystają biblioteki w regionie. W takiej okoliczności niezbędne będzie przez bibliotekę wojewódzką prowadzenie rejestru kategorii przetwarzanych danych.

W rozdziale 6.6. zamieszczono przykładową tabelę dla rejestru kategorii czynności przetwarzania.

6.5. Krajowe Ramy Interoperacyjności i System Zarządzania Bezpieczeństwem Informacji.

Ochrona danych osobowych w bibliotece polegająca w dużej mierze na realizacji przepisów RODO i Ustawy ODO nie może być realizowana w oderwaniu od realizacji obowiązku prawnego wynikającego z innych aktów normatywnych. W niektórych przypadkach obowiązki nałożone na bibliotekę mocą różnych ustaw są do siebie podobne, np. obowiązek przeprowadzania analizy ryzyka wynika zarówno z ustawy o finansach publicznych, jak również z przepisów RODO (kwestia ta została szczegółowo omówiona w rozdziale 7 niniejszego Kodeksu). Opieranie działań na różnych aktach prawnych jest również realizowane w zakresie prawa pracy. W bibliotece są pobierane dane od kandydatów do pracy i pracowników na podstawie ustawy Kodeks pracy, jednocześnie realizowany jest obowiązek informacyjny na podstawie przepisów RODO. Zrozumienie takiego sposobu

działania jest bardzo istotne w kontekście właściwego wdrożenia w bibliotece Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

Wprowadzenie uregulowań prawnych w zakresie SZBI rozpoczęło się od wejścia w życie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne. Przyczyną uchwalenia tego aktu prawnego było postępujące wprowadzanie nowych technologii do instytucji publicznych, w tym także do bibliotek, przy jednoczesnym wzroście zagrożeń wynikających przede wszystkim z wykorzystania sieci Internet. Jednym z kilkudziesięciu aktów wykonawczych do ustawy było rozporządzenie, na mocy którego wprowadzono m.in. tzw. Krajowe Ramy Interoperacyjności (KRI) oraz minimalne wymagania dla systemów teleinformatycznych. KRI to zbiór wytycznych (wymagań) odnoszących się do systemów informatycznych, dzięki którym mają one docelowo charakteryzować się interoperacyjnością. Oznacza to, że będą kompatybilne z innymi systemami i będzie możliwa współpraca pomiędzy systemami różnych instytucji. Takie regulacje zostały stworzone w dużej mierze z myślą o urzędach realizujących zadania publiczne na rzecz obywateli, dzięki czemu powinno usprawnić się ich funkcjonowanie, a osoby korzystające z ich usług powinny zaoszczędzić czas, np. z powodu braku konieczności uzyskania zaświadczenia w „urzędzie A" w celu załatwienia sprawy w „urzędzie B", z uwagi na to, że urzędnik sam pobierze informacje z odpowiedniego rejestru publicznego. Ustawodawca uchwalając wskazany akt prawny, jak również Rada Ministrów wydając rozporządzenie nie doprecyzowali jednak katalogu instytucji, które podlegają tym regulacjom. W związku z tym przepisy w praktyce muszą zostać wdrożone przez wszystkie podmioty realizujące zadania publiczne, w tym biblioteki. Podczas szkoleń i konsultacji kadra kierownicza bibliotek regularnie zwraca uwagę na problemy z realizacją omawianych przepisów prawa, ze szczególnym uwzględnieniem:

- braku szczegółowych wytycznych dla bibliotek i innych instytucji kultury,
- niezrozumiałej siatki pojęciowej zawartej w aktach prawnych,
- braku odpowiednio przygotowanej kadry do zapewnienia KRI i innych wymogów w bibliotekach.

Biorąc pod uwagę wskazane mankamenty warto podejść do zagadnień związanych z KRI i wdrażać przepisy prawa stopniowo i w taki sposób, żeby nowe rozwiązania rzeczywiście przyczyniły się do poprawy bezpieczeństwa informacji w bibliotece. Najbardziej istotny z punktu widzenia ochrony danych osobowych jest §20. wskazanego rozporządzenia, na mocy którego podmiot realizujący zadania publiczne „opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność". W §20. określono także szeroki katalog działań, jakie powinny zostać podjęte w celu zapewnienia SZBI. Jednym z nich jest „zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok". Warto jednak zwrócić szczególną uwagę na pkt 3 zawarty w §20. rozporządzenia wprowadzającego KRI, zgodnie z którym wymagania te „uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą". Oznacza to, że efektywnym rozwiązaniem w zakresie wdrożenia wskazanego w podrozdziale 6.5. wymogu prawnego jest stopniowe wdrażanie w bibliotece normy PN-ISO/IEC 27001. W tym kontekście warto, aby nawet początkujący IOD wraz ze swoim rozwojem zawodowym i zwiększaniem zakresu swoich kompetencji zdobywał również wiedzę w zakresie wskazanej Normy.

Jednocześnie należy podkreślić, iż w przypadku bibliotek, które jeszcze nie wdrożyły wymagań zawartych w rozporządzeniu wprowadzającym KRI, nie należy tego działania jedynie odkładać na przyszłość. W przypadku realizacji przepisów RODO i Ustawy ODO bierne pozostawienie tego obszaru nie będzie zresztą możliwe. Wynika to z faktu, iż Grupa Robocza Art. 29. (zastąpiona od

25 maja 2019 r. Europejską Radą Ochrony Danych), która przygotowywała poszczególne przepisy RODO opierała się przy tworzeniu poszczególnych rozwiązań na międzynarodowej Normie ISO/IEC 27001, która zawiera standardy w zakresie SZBI. Polski Komitet Normalizacyjny opublikował w Polsce Normę pod nazwą PN-ISO/IEC 27001:2007 i jest to ta sama Norma, którą wskazano w omawianych aktach prawnych wprowadzających KRI. Podsumowując, przepisy RODO są zgodne ze wskazanymi Normami, a fragmentarycznie stanowią ich wierną implementację. W bibliotekach, w których wdrażane jest RODO jest jednocześnie wdrażane szerokie spektrum elementów SZBI.

Należy jednak podkreślić, iż samo wdrażanie przepisów RODO i ustawy ODO, nawet w przypadku postępowania w najszerszym zakresie zgodnie z wytycznymi zawartymi w niniejszym Kodeksie nie oznacza pełnego wdrożenia SZBI. Wynika to przede wszystkim z faktu, iż SZBI ma szerszy zakres niż ochrona danych osobowych. Poprzez przepisy RODO i ustawy ODO uregulowano bowiem kwestię przetwarzania danych osób fizycznych, zidentyfikowanych lub w przypadku których taka identyfikacja jest możliwa. SZBI to natomiast system, który ma na celu ochronę wszystkich informacji, którym można nadać atrybut poufności. Oznacza to, że z różnych względów powinny stanowić tajemnicę. Jeżeli np. zostaje ogłoszone postępowanie o zamówienie publiczne, a stroną ogłaszającą jest biblioteka, to zgłaszające się podmioty mogą w praktyce składać dokumenty, które tylko w minimalnym stopniu zawierają dane osobowe. Ich poufność będzie natomiast wynikała z innej przyczyny – w przypadku przytoczonego przykładu będzie to konieczność zachowania tajemnicy w zakresie szczegółów oferty, żeby uniemożliwić innym oferentom nieuczciwe przebicie takiej oferty.

W praktyce SZBI w bibliotece powinien opierać się na uporządkowaniu wszystkich dotychczas opracowanych procedur w instytucji. Jednym z najbardziej istotnych elementów dokumentacji Systemu jest spis treści. To właśnie tam należy wskazać wszystkie procedury, regulaminy i inne ważne dokumenty stanowiące wewnętrzne regulacje prawne funkcjonowania jednostki. Z bezpieczeństwem informacji wiąże się bowiem niemal wszystko, co jest związane z funkcjonowaniem biblioteki, np. procedury ppoż., których efektywna realizacja pomaga uniknąć utraty informacji spowodowanej pożarem. Tworzenie Systemu można zatem rozpocząć od stworzenia schematu, w którym grupuje się wszystkie dokumenty. Jednocześnie można wtedy, analizując stworzoną wizualizację, zdiagnozować tzw. obszary deficytowe, co oznacza znalezienie obszarów poddanych niewłaściwym regulacjom. W praktyce funkcjonowania bibliotek znane są sytuacje, w których podczas inwentaryzacji procedur w celu wpisania ich do spisu treści SZBI dyrekcja dostrzegała braki w dokumentach, np. poprawnie sporządzony regulamin kontroli zarządczej, jednak bez opracowanych niektórych załączników.

Dopiero po dokładnej inwentaryzacji dotychczas funkcjonujących procedur w bibliotece, możliwe jest rozważenie przygotowania nowych dokumentów. Priorytetowe znaczenie z punktu widzenia SZBI mają polityki bezpieczeństwa informacji, stanowiące opis wszystkich działań, mających na celu ochronę informacji (nie tylko ochronę danych osobowych). Jednocześnie, zgodnie z informacjami zawartymi w niniejszym podrozdziale, warto przyjąć SZBI przede wszystkim jako proces porządkujący dotychczasowe procedury oraz strategię ich zmiany w celu zwiększenia efektywności ochrony informacji.

6.6. Dobre praktyki, wytyczne i wskazówki.

W rozdziale 6.3. zostały omówione wymagania dotyczące rejestru czynności przetwarzania Poniższa tabela (Tabela 1) stanowi przykład rejestru czynności przetwarzania. Przestawiona tabela zawiera wszystkie pola, które wymagane są zgodnie z przepisami RODO.

Tabela 1. Rejestr czynności przetwarzania – wersja podstawowa

ADMINISTRATOR DANYCH OSOBOWYCH NAZWA + ADRES INSPEKTOR OCHRONY DANYCH OSOBOWYCH							
Czynność przetwarzania (nazwa zbioru/operacja przetwarzania)	Opis kategorii osób, których dane dotyczą	Cel przetwarzania	Kategoria danych osobowych przetwarzanych w ramach czynności	Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione	Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej	Planowany termin usunięcia danych	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa

Powyższą tabelę można dowolnie modyfikować i dodawać elementy, które administrator uzna za istotne. Przykładem rozszerzenia rejestru o dodatkowe pola jest Tabela 2. Takie rozszerzenie stanowi dobrą praktykę.

Tabela 2. Rejestr czynności przetwarzania – wersja rozszerzona

ADMINISTRATOR DANYCH OSOBOWYCH NAZWA + ADRES INSPEKTOR OCHRONY DANYCH OSOBOWYCH												
Czynność przetwarzania (nazwa zbioru/ operacja przetwarzania)	Opis kategorii osób, których dane dotyczą	Cel przetwarzania	Podstawa prawna	Nazwy programów	Nazwy pól informacyjnych	Kategoria danych osobowych przetwarzanych w ramach czynności	Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione	Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej	Planowany termin usunięcia danych	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa		

Przykładowy rozszerzony rejestr kategorii czynności przetwarzania uzupełniony o dodatkowe pola.

Tabela 3. Rejestr kategorii czynności przetwarzania – wersja rozszerzona.

PODMIOT PRZETWARZAJCY NAZWA + ADRES INSPEKTOR OCHRONY DANYCH OSOBOWYCH										
Administrator Danych Osobowych (nazwa)	Adres ADO	Data zawarcia umowy	Data zakończenia umowy	Sposób pozyskania danych	Opis czynności po wygaśnięciu umowy powierzenia	Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione	Cel przetwarzania przez podmiot przetwarzający	Podstawa prawna	Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa

Przykładowy rejestr kategorii czynności przetwarzania danych

Tabela 4. Rejestr kategorii czynności przetwarzania – wersja podstawowa

PODMIOT PRZETWARZAJĄCY NAZWA + ADRES INSPEKTOR OCHRONY DANYCH OSOBOWYCH				
Administrator Danych Osobowych (nazwa)	Adres ADO	Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione	Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa

Procedura archiwizacji kart zobowiązań

1. Konta użytkowników biblioteki są poddawane okresowym przeglądom pod kątem aktywności korzystania użytkowników z biblioteki w terminie do końca lutego danego roku.
2. Karty zobowiązań użytkowników, którzy nie korzystają z biblioteki od co najmniej dwóch lat licząc od końca drugiego pełnego roku nieaktywności, są przenoszone do składnicy akt w terminie do końca marca danego roku.
3. Przeniesione do składnicy akt karty zobowiązań są przechowywane w niej przez kolejne trzy lata licząc łącznie z rokiem przeniesienia karty zobowiązania do składnicy.
4. Karta zobowiązania użytkownika, który ponownie rozpocznie korzystanie z biblioteki, zostaje przeniesiona ze składnicy akt do dokumentacji podręcznej.
5. Karty zobowiązań użytkowników, którzy nie wznowili korzystania z biblioteki, podlegają brakowaniu na zasadach określonych w przepisach kancelaryjno-archiwalnych biblioteki.

Komentarz
Przyjęto pięcioletni okres przechowywania danych użytkowników biblioteki.

7 INSPEKTOR OCHRONY DANYCH (IOD) W BIBLIOTECE

7.1. Obowiązek powołania IOD w bibliotece.

Zgodnie z art. 37 ust. 1 RODO administrator wyznacza IOD zawsze, gdy przetwarzania dokonuje organ lub podmiot publiczny, w szczególności biblioteka. Warto także zwrócić uwagę na kwestię bibliotek pozostających w strukturach innych podmiotów, jak biblioteka szkolna, akademicka, w ramach ośrodka kultury. IOD jest wówczas wyznaczany dla całego podmiotu. Podmioty publiczne są uprawnione do wyznaczenia jednego inspektora. Administratorzy podejmujący taką decyzję, powinni uwzględnić wielkość, strukturę a także skalę przetwarzania w grupie podmiotów w kontekście możliwości skutecznej realizacji ustawowych obowiązków inspektora.

Biorąc pod uwagę fakt, że przetwarzanie danych osobowych w sposób niezgodny z przepisami może narazić bibliotekę na karę finansową w wysokości nawet 10 000 zł, wyznaczenie IOD, którego obowiązkiem jest monitorowanie zgodności przetwarzania danych z przepisami, jest racjonalnym działaniem, mającym na celu minimalizację ryzyk dla ochrony danych przetwarzanych w bibliotece. Inspektor pomaga dyrektorowi wdrożyć w bibliotece rozwiązania umożliwiające podniesienie poziomu bezpieczeństwa przetwarzania danych i zapewnienie zgodności z obowiązującymi przepisami.

Dyrektor biblioteki dokonuje subiektywnej oceny kwalifikacji inspektora, ponieważ w przepisach nie wskazano konkretnych wymagań w zakresie jego wiedzy i doświadczenia. Ocena kompetencji inspektora powinna w szczególności polegać na teście wiedzy z przepisów o ochronie danych osobowych, a także przepisów szczególnych dotyczących działalności biblioteki. Brak znajomości przepisów sektorowych będzie stanowił barierę w skutecznym i właściwym doradzaniu dyrektorowi biblioteki w wypełnianiu jego obowiązków wynikających z RODO. Należy także zwrócić uwagę na cechy osobowości IOD, ponieważ powinna to być osoba odznaczająca się silnym kręgosłupem moralnym oraz kierująca się w wykonywaniu swoich obowiązków etyką zawodową. Sposób prowadzenia przez nią komunikacji z czytelnikami, powinien być adekwatny do poziomu standardowej komunikacji z odbiorcami usług biblioteki.

Wyznaczenie IOD powinno nastąpić w formie zarządzenia lub innego dokumentu zawierającego formułę wyznaczenia do pełnienia funkcji inspektora w bibliotece. Podstawą prawną wyznaczenia IOD są art. 37 ust. 1 RODO oraz art. 8 ustawy ODO. Inspektor powinien na piśmie potwierdzić wyznaczenie na to stanowisko oraz nowe obowiązki. Strona formalna wyznaczenia IOD jest ważna, ze względu na obowiązek z art. 10 ust. 1 ustawy ODO zawiadomienia Prezesa UODO w ciągu 14 dni od daty wyznaczenia. Zawiadomienie powinno zawierać imię, nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora. Wskazane dane powinny być danymi służbowymi. Należy pamiętać, iż administrator zobowiązany jest również zgodnie z art. 10 ust. 4 ustawy ODO do zawiadamiania Prezesa UODO o każdej zmianie danych inspektora oraz o jego odwołaniu.

Ustawodawca w art. 11a ust. 1 ustawy ODO przewidział możliwość wyznaczenia zastępcy inspektora w czasie jego nieobecności. Osoba zastępująca musi jednak spełniać te same kryteria jakie dotyczą IOD a także ponosi tę samą odpowiedzialność przed administratorem. Jej dane także powinny zostać przekazane do wiadomości Prezesa UODO. Wszystkie zawiadomienia dokonuje się elektronicznie, uwierzytelniając je podpisem kwalifikowanym lub profilem zaufanym (ePUAP). Dodatkowo zgodnie z art. 11 ustawy ODO dyrektor biblioteki zobowiązany jest do udostępnienia danych IOD w zakresie imienia i nazwiska oraz danych kontaktowych w zakresie numeru telefonu lub adresu e-mail na stronie internetowej biblioteki. Należy podkreślić, że wypełniając obowiązek informacyjny wobec osoby, której dane dotyczą, na zasadach określonych w art. 13 i 14 RODO, administrator jest zobligowany podać jedynie dane kontaktowe do inspektora. Jest to związane z praktycznym aspektem aktualizacji wszystkich obowiązków informacyjnych, jeżeli zmieni się inspektor. Przyjętą praktyką jest wskazywanie ogólnego adresu e-mail do inspektora, np. iod@nazwabiblioteki.pl, co umożliwia łatwiejszy kontakt.

7.2. Formy współpracy z IOD.

Możliwe formy współpracy administratora z IOD zostały określone w art. 37 ust. 6 RODO, zgodnie z którym może on być zarówno członkiem personelu administratora (czyli związany stosunkiem pracy), jak i wykonywać zadania na podstawie umowy o świadczenie usług (czyli związany stosunkiem cywilnoprawnym). W sytuacji, gdy dyrektor biblioteki zdecyduje się wybrać IOD wśród pracowników, stosunek prawny jaki będzie łączyć strony umowy regulowany będzie w oparciu o przepisy prawa pracy. Najczęstszym rozwiązaniem ze względów finansowych jest wyznaczenie inspektora spośród kadry pracowników aktualnie zatrudnionych w bibliotece poprzez „dodanie" nowych obowiązków pracownikowi, który taką funkcję będzie w stanie realizować. Jest to rozwiązanie dopuszczalne zgodnie z art. 38 ust. 6 RODO. Pozytywnym aspektem takiego rozwiązania jest znajomość specyfiki pracy jednostki, a także to, że IOD jest osobą zaufaną i sprawdzoną, a jego wyznaczenie nie generuje nadmiernych kosztów. Wśród ryzyk takiego rozwiązania należy wskazać ryzyko konfliktu interesów w sytuacji, gdy pracownik wykonuje inne zadania, w których przetwarza się dane osobowe (a jako IOD powinien kontrolować zgodność ich przetwarzania z przepisami) oraz ryzyko słabego przygotowania merytorycznego i niskiej wiedzy fachowej. Wobec wskazanych ryzyk, lepszym rozwiązaniem jest zatrudnienie nowej osoby lub faktyczna, rzeczywista redukcja etatu wyznaczonego wśród pracowników inspektora i wyznaczenie jego zastępcy, który będzie monitorował obszary przetwarzania, w których występuje konflikt interesu.

Drugą dostępną formą współpracy jest możliwość świadczenia usługi przez zewnętrznego inspektora na podstawie umowy cywilnoprawnej. Zaletą takiego rozwiązania jest możliwość znalezienia inspektora z należytą wiedzą i doświadczeniem w zakresie ochrony danych, a niewątpliwą wadą utrudniony kontakt, problem z dyspozycyjnością oraz ryzyka jakie są związane z przekazywaniem osobie spoza jednostki informacji dotyczących funkcjonowania systemu ochrony informacji. Osoba taka, co zrozumiałe nie będzie również na początku znać specyfiki działania ADO.

Dobrym rozwiązaniem, z punktu widzenia biblioteki, jest wyznaczenie jednego IOD dla kilku podmiotów (art. 37 ust. 3 RODO). W takim przypadku każda z jednostek o podobnej strukturze organizacyjnej oraz specyfice działania, wyznacza osobę, która staje się inspektorem dla każdej jednostki z osobna. Elementem wiążącym IOD z poszczególnymi jednostkami powinno być jego wyznaczenie przez każdego dyrektora placówki jako administratora danych osobowych zgodnie z artykułem 37 ust. 1 RODO. W oparciu o takie wyznaczenie, a co za tym idzie zawiadomienie organu nadzorczego

oraz opublikowanie danych kontaktowych IOD zgodnie z artykułem 37 ust. 7 RODO wynika realizacja działań IOD. Jednocześnie w sytuacji, gdy administratorzy współpracują ze sobą, jest o wiele mniejsze ryzyko braku kontaktu z IOD, jak przy całkowicie zewnętrznym specjaliście. W praktyce jest to rozwiązanie, które stosują wspólnie szkoły, przedszkola i biblioteki.

Istotną kwestią, która powinna determinować wybór formy zatrudnienia inspektora w bibliotece jest zakres jego odpowiedzialności w sytuacji, gdy administrator poniesie szkodę, np. z tytułu administracyjnej kary pieniężnej. O ile zakres odpowiedzialności pracownika uzależniony jest od strony podmiotowej czynu, czyli jego umyślności lub nieumyślności (a tę należy najpierw udowodnić, bo od niej zależy ewentualna wysokość odszkodowania za szkodę pracodawcy), o tyle odpowiedzialność usługodawcy działającego w oparciu o umowę cywilnoprawną może być precyzyjnie uregulowana zapisami umowy co może skutkować całkowitym przeniesieniem odpowiedzialności za ewentualne błędy w realizacji zobowiązań na podmiot zewnętrzny. Administrator danych i inspektor w łączącej ich umowie cywilnoprawnej mogą ułożyć stosunek prawny według własnego uznania. Odpowiedzialność IOD za wykonywane czynności wynikające z umowy oparta będzie na przepisach art. 471 Kodeksu cywilnego, w zakresie naprawienia szkody wynikłej z niewykonania lub nienależytego wykonania zobowiązania. W prawnie uzasadnionym interesie administratora przy zawieraniu umowy na świadczenie usług IOD, jest obowiązek wykonywania zadań przez osobę będącą stroną umowy bez możliwości dalszego zlecania.

7.3. Rola i status IOD.

Rolą inspektora ochrony danych jest zapewnienie nadzoru nad zgodnością przetwarzania danych osobowych w bibliotece z przepisami o ochronie danych osobowych, a także dążenie do zapewnienia tej zgodności przez administratora. Ze względu na ścisłe powiązanie przetwarzania danych osobowych z innymi rodzajami informacji, związanymi z działalnością jednostki, jej tajemnicami czy wręcz informacjami chronionymi z innych ustaw (np. dane medyczne, informacje niejawne, tajemnice zawodowe) IOD w praktyce często nadzoruje cały system ochrony informacji w jednostce. Nie da się stosować procesowego podejścia do przetwarzania danych, nie biorąc pod uwagę innych czynników wpływających na ryzyka i zagrożenia dla ochrony danych osobowych. Właśnie dlatego administrator zapewnia inspektorowi, zgodnie z art. 38 RODO, wgląd we wszystkie sprawy dotyczące przetwarzania danych, w tym dostęp do danych osobowych i wszelkich operacji na nich, a także zasoby niezbędne do wykonywania zadań, w szczególności do utrzymania wiedzy fachowej. Przepisy RODO podkreślają niezależność IOD, w szczególności, aby wyeliminować próby ewentualnych nacisków na inspektora, art. 38 ust. 3 RODO określa: „administrator zapewnia by inspektor nie otrzymywał instrukcji dotyczących wykonywania zadań, a także nie może być karany ani odwołany za ich wypełnianie". W konsekwencji tego przepisu, administrator nie może karać ani odwołać IOD w przypadku, gdy realizuje on swoje zadania w sposób zgodny z umową i przepisami powszechnie obowiązującego prawa.

Status inspektora jest podkreślony również poprzez fakt, iż musi on podlegać bezpośrednio najwyższemu kierownictwu administratora czyli dyrektorowi placówki. W związku z powyższym bardzo trudnym w realizacji wydaje się zapewnienie owej niezależności pracownikowi, który wykonuje również inne zadania i podlega w tym względzie kierownictwu średniego szczebla.

Inspektor jest wyznaczany w bibliotece w celu wspierania jej dyrektora w prawidłowym realizowaniu obowiązków wynikających z przepisów o ochronie danych osobowych. Jego rolą jest monitorowanie procesów przetwarzania w zakresie zgodności z przepisami RODO, wydawanie zaleceń,

doradzanie, szkolenie personelu. Nie odpowiada za zapewnienie zgodności przetwarzania danych z RODO, a także nie odpowiada za wdrażanie i stosowanie rozwiązań, które mają zapewnić właściwe stosowanie przepisów RODO – to są niezbywalne obowiązki dyrektora biblioteki, wynikające wprost z przepisów prawa. Inspektor nie podejmuje decyzji dotyczących sposobów przetwarzania danych w bibliotece, nie może narzucić dyrektorowi konkretnych rozwiązań i działań. Jest on ciałem doradczym i wspierającym.

Inspektor jest niezależny w swoich działaniach i nie powinien być poddawany naciskom ze strony dyrektora lub innych pracowników. Dyrektor nie może odwołać ani ukarać administratora wypełnianie przez niego ustawowych zadań. Oznacza to, że jest on uprawniony do wskazywania naruszeń i niewłaściwych praktyk dotyczących przetwarzania danych, a także dokumentowania ich, w szczególności w swoim sprawozdaniu ze sprawdzenia. Rolą inspektora jest znajdowanie słabości systemu ochrony danych w bibliotece i wskazywanie, problemów oraz zagrożeń dla ochrony danych, a następnie przekazywanie administratorowi zaleceń w celu przywrócenia stanu zgodnego z przepisami prawa. Dyrektor biblioteki ma zapewnić właściwą ochronę danych osobowych, więc do niego należy obowiązek zastosowania właściwych środków ochrony. Istotne w relacji inspektor – dyrektor jest podejmowanie dialogu w celu osiągnięcia skutecznych rozwiązań.

7.4. Zadania IOD.

Zadania inspektora zostały określone w art. 39 RODO. Przede wszystkim pełni on rolę wspierającą administratora w zapewnieniu zgodności przetwarzania danych z przepisami o ochronie danych osobowych.

Jednym z ważniejszych obowiązków IOD jest informowanie pracowników, podmiotu przetwarzającego oraz administratora o obowiązkach wynikających z przepisów ochrony danych osobowych. Przepisy RODO wyraźnie wskazują na konieczność posiadania przez IOD wysokich kwalifikacji i wiedzy, nie tylko w zakresie przepisów RODO, ale przede wszystkim przepisów sektorowych, dzięki czemu działania realizowane przez niego będą mieć wpływ na bezpieczeństwo funkcjonowania jednostki w zakresie jej ochrony fizycznej, technicznej i organizacyjnej. Ich realizacja opiera się na monitorowaniu przestrzegania przepisów, czyli prowadzeniu audytów sprawdzających w jakim zakresie w jednostce przestrzegane są przepisy określone w RODO oraz innych ustawach na podstawie, których działa biblioteka, jak przepisy biblioteczne, prawo pracy, czy przepisy regulujące dostęp do informacji publicznej. W zakresie tego uprawnienia, IOD zobowiązany jest do przeprowadzania audytów wewnątrz jednostki, które mają na celu weryfikację wdrożonych rozwiązań w oparciu o wcześniej przeprowadzoną analizę ryzyka, a w konsekwencji przedstawienie administratorowi sprawozdań, w których zawarte powinny być propozycje ewentualnych działań naprawczych.

Ze względu na charakter i zakres danych osobowych przetwarzanych w bibliotece wydaje się, że nie będzie zachodzić potrzeba przeprowadzania oceny skutków przez administratora, a tym samym udzielania przez IOD zaleceń w tym zakresie. Działania takie wynikają z zapisów art. 35 ust. 1 RODO mówiących o wysokim ryzyku naruszenia praw lub wolności osób których dane dotyczą co w sytuacji przetwarzania danych w standardowych procesach w bibliotece nie powinno mieć miejsca.

Bardzo istotnym elementem pracy inspektora jest pełnienie roli punktu kontaktowego dla osób, których dane dotyczą w celu realizacji ich praw (art. 38 ust. 4 RODO) w związku z powyższym jego dane kontaktowe powinny być dostępne na stronie internetowej oraz we wszystkich klauzulach informacyjnych biblioteki. Ponadto IOD jest punktem kontaktowym dla Prezesa UODO i zobowiązany jest do współpracy z organem nadzorczym w zakresie wszystkich zadań, za które jest odpowiedzialny, a także wszelkich innych obowiązków wynikających z RODO.

Katalog czynności realizowanych przez inspektora jest otwarty i poza powyższymi opisanymi w RODO można uznać że na polecenie administratora IOD może wykonywać inne zadania wynikające z RODO. Mogą to być działania wspierający przy:

- prowadzeniu rejestru czynności przetwarzania oraz rejestru kategorii czynności przetwarzania, rozumiane jako zebranie niezbędnych informacji i fizyczne utworzenie oraz aktualizowanie na ich podstawie rejestru,
- zgłaszaniu naruszeń do organu nadzorczego, rozumiane jako czynność techniczna,
- prowadzeniu ciągłej analizy ryzyka dla wszystkich procesów zapisanych w rejestrze czynności przetwarzania, rozumiane jako szacowanie ryzyka na podstawie przeprowadzonych audytów lub informacji uzyskanych od personelu i dyrektora.

Należy jednakże pamiętać, że dyrektor biblioteki nie może zupełnie przerzucić na inspektora odpowiedzialności za realizowanie tych czynności, a jedynie uczynić go koordynatorem, który pomoże w prowadzeniu tych działań. W przypadku każdej z tych czynności, ostateczne zatwierdzenie i podjęcie działań jest obowiązkiem dyrektora biblioteki.

7.5. Dobre praktyki, wytyczne i wskazówki.

I. Jeden IOD dla grupy podmiotów.

Jeżeli w całej gminie został wyznaczony jeden inspektor, to wydaje się niemożliwe, aby był w stanie skutecznie monitorować zgodność przetwarzania danych we wszystkich jej jednostkach organizacyjnych. Takie rozwiązanie ma szansę powodzenia jedynie wówczas, gdy każdy z administratorów wyznaczy u siebie osobę (koordynatora) odpowiedzialną za wypełnianie poleceń i zaleceń IOD. Wówczas inspektor za pośrednictwem koordynatorów uzyskuje niezbędne informacje do zapewnienia stałego monitorowania zgodności przetwarzania z przepisami, a także może być w stanie uczestniczyć w wielu postępowaniach dotyczących przetwarzania danych u różnych administratorów, jednocześnie. Wyznaczenie jednego inspektora dla grupy podmiotów publicznych, łączy się też z ryzykiem, że będzie on ustalał priorytety działania, adekwatne do poziomu ryzyk i zagrożeń dla danych. Wydaje się oczywiste, że w pierwszej kolejności skupi się na urzędzie gminy, następnie szkołach i ośrodku pomocy społecznej. Biblioteka będzie jednym z najmniej istotnych priorytetów na jego liście. Bardziej rekomendowanym rozwiązaniem jest wyznaczenie IOD dla grupy podobnych podmiotów, np. bibliotek w ramach jednego powiatu.

II. Test wiedzy IOD.

Dyrektor w celu zbadania kompetencji kandydata na inspektora może zapytać go o kwestie bezpośrednio wynikające z RODO, np. jakie są zasady przetwarzania danych osobowych (art. 5 RODO), jakie czynności na danych osobowych są ich przetwarzaniem; czy przechowywanie danych to także przetwarzanie (art. 4 RODO), czy zgodna na przetwarzanie danych zawsze jest niezbędna (art. 6), jak należy realizować żądania osoby, której dane dotyczą wynikające z RODO (art. 12 RODO, a potem w zależności od żądania 13-22 RODO), czy w każdych okolicznościach przysługuje prawo do bycia zapomnianym (art. 17 RODO), jak należy dokonywać doboru środków bezpieczeństwa do ryzyk i zagrożeń dla ochrony danych (art. 32 RODO), itd.

Należy także zadać pytania dotyczące podstawowego zakresu działalności biblioteki oraz ustawy o bibliotekach, np. czy czytelnik musi wyrażać zgodę na przetwarzanie jego danych do korzystania z biblioteki, czy biblioteka musi prosić czytelnika o zgodę na windykację, jakie dane biblioteka musi zbierać na potrzeby statystyczne, itp.

III. Przykłady konfliktu interesów w przypadku IOD wyznaczonego wśród członków personelu.

Sekretarz jest osobą zaangażowaną w większość procesów przetwarzania w bibliotece. Jest pośrednikiem w większości procesów związanych z zawieraniem umów, windykacją, porządkowaniem dokumentów, itd. Jest też bardzo silna zależność służbowa pomiędzy sekretarzem a dyrektorem biblioteki, co utrudnia spełnienie warunku niezależności, pomimo tego, że w strukturze organizacyjnej, podlega on bezpośrednio pod dyrektora.

Informatyk jest osobą odpowiedzialną za zapewnienie bezpieczeństwa informatycznego. Jego wiedza w tym zakresie nie oznacza, że jest on specjalistą w zakresie ochronnych danych osobowych, więc wyznaczenie go na to stanowisko, musi być poparte przeprowadzeniem rzeczowej analizy w tym zakresie. Dodatkowo, jeżeli jest to osoba odpowiedzialna za zapewnienie ochrony danych przetwarzanych w systemach informatycznych, w szczególności systemie bibliotecznym oraz kadrowo-księgowym, nie będzie w stanie zapewnić skutecznego nadzoru (audytu) tej strefy przetwarzania danych.

Główny księgowy jest osobą, którego zakres odpowiedzialności i obowiązków jest zbyt duży, aby móc połączyć go z rolą IOD. Nie będzie w stanie obiektywnie monitorować zgodności przetwarzania z przepisami.

Księgowy jest osobą, która przetwarza dane osobowe w bardzo szerokim zakresie, odpowiada za realizację jednych z najważniejszych procesów przetwarzania w bibliotece. Nie jest w stanie obiektywnie ocenić zgodności przetwarzania z przepisami.

8 ANALIZA RYZYKA I OCENA SKUTKÓW DLA OCHRONY DANYCH

8.1. Podstawa prawna i cele analizy ryzyka w bibliotece.

Analiza ryzyka to proces, który systematycznie zyskuje na znaczeniu i staje się wykładnikiem nowoczesnego zarządzania. Może dotoczyć wielu dziedzin związanych z funkcjonowaniem firm i instytucji. W wymiarze ogólnym analiza ryzyka opiera się najczęściej na podobnym schemacie działania. Na początku wyznaczane są cele, zbiory, działania, procesy lub inne obszary co do których szacowane będzie ryzyko. Następnie osoba przeprowadzająca analizę musi określić, jakie perturbacje mogą się wydarzyć i jak bardzo prawdopodobne jest, że zostanie zakłócone to, co zostało zaplanowane. W dalszym etapie należy określić czy analizowana sytuacja może zostać zaakceptowana, czy też należy wprowadzić środki zapobiegające jej wystąpieniu.

W przypadku firm analiza ryzyka miała do 25 maja 2018 r. najczęściej charakter dobrej praktyki. Nie była działaniem obowiązkowym, jednak przedsiębiorcy chętnie sięgali po to narzędzie, ponieważ umożliwia ono maksymalizację zysków poprzez eliminację zagrożeń jeszcze przed ich wystąpieniem lub na jego wczesnym etapie. Natomiast w przypadku bibliotek i innych instytucji publicznych zaczęto stopniowo wprowadzać obowiązek prawny analizy ryzyka. Przykładem w tym zakresie jest obowiązek spoczywający na pracodawcy, który zgodnie z art. 226 Kodeksu pracy musi ocenić i udokumentować „ryzyko zawodowe związane z wykonywaną pracą oraz stosuje niezbędne środki profilaktyczne zmniejszające ryzyko". Analiza ryzyka została także usankcjonowana w związku z Krajowymi Ramami Operacyjności i Systemem Zarządzania Bezpieczeństwem Informacji, co zostało omówione w podrozdziale 6.5. niniejszego Kodeksu. Jednak kluczowe znaczenie w rozwoju i upowszechnieniu analizy ryzyka w instytucjach publicznych ma system kontroli zarządczej. Obowiązek wdrożenia tego systemu pojawił się 1 stycznia 2010 r. wraz z wejściem w życie ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych. Wówczas w bibliotekach rozpoczęto wieloaspektową analizę ryzyka, która przy prawidłowej realizacji powinna dotyczyć wszystkich kluczowych obszarów funkcjonowania instytucji. Analiza ta sprawiała kadrze kierowniczej i pracownikom bibliotek trudności, ponieważ wraz z wprowadzeniem obligatoryjnego charakteru wdrożenia systemu kontroli zarządczej zabrakło szkoleń i precyzyjnego wskazania jak należy to poprawnie realizować. W konsekwencji opracowano wytyczne, które ukazały się w formie Komunikatu nr 6 Ministra Finansów[5]. Zbiór wytycznych stał się jednym z najbardziej wartościowych opracowań w zakresie planowania i zarządzania ryzykiem, jakie są obecnie dostępne. Może stanowić wartościowe źródło wiedzy dla wszystkich osób zajmujących się analizą ryzyka, nie tylko w zakresie kontroli zarządczej i nie tylko w instytucjach publicznych.

[5] Komunikat nr 6 Ministra Finansów z dnia 6 grudnia 2012 r. w sprawie szczegółowych wytycznych dla sektora finansów publicznych w zakresie planowania i zarządzania ryzykiem.

Wejście w życie przepisów RODO skutkowało znaczącymi zmianami w zakresie przeprowadzania analizy ryzyka. Każdy ADO ma obecnie obowiązek takiego działania. W przypadku bibliotek oznacza to konieczność wykonywania dodatkowych czynności, ponieważ nie można uznać, iż analiza ryzyka prowadzona w związku z realizacją kontroli zarządczej stanowi realizację przepisów RODO. Warto jednak pamiętać, żeby:

- obydwie analizy ryzyka były ze sobą spójne, nawet jeśli ich przeprowadzaniem zajmują się różni pracownicy (zagrożenia powinny być szacowane na podobnym poziomie),
- zastosować w miarę możliwości podobne kryteria szacowania ryzyka (przykładowe kryteria zostały przedstawione w podrozdziale 8.2.),
- w przypadku wystąpienia ryzyka średniego lub wysokiego (a w niektórych przypadkach również niskiego) zaproponować podobne mechanizmy naprawcze.

Jako podstawę prawną analizy ryzyka należy wskazać art. 32 ust. 2 RODO, w którym wskazano, iż „oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych". Należy jednak podkreślić, iż przepisy RODO odnoszą się do analizy ryzyka w szerszym zakresie. Wielokrotnie zwrócono uwagę m.in. na „ryzyko naruszenia praw lub wolności osób fizycznych" oraz ograniczaniu ryzyka poprzez zastosowanie pseudonimizacji. Dlatego warto dokonywać wykładni przepisów RODO w możliwie jak najszerszym zakresie. Analiza ryzyka bez wątpienia nie jest wyłącznie jedną z administracyjnych czynności polegających na wypełnianiu kwestionariuszy i powtarzaniu tego działania cyklicznie. Intencją twórców RODO jest natomiast zmiana podejścia każdego ADO do ochrony danych osobowych. Zadaniem kadry kierowniczej i pracowników bibliotek jest zatem opieranie wszystkich działań związanych z ochroną danych osobowych na analizie ryzyka związanego z naruszeniem poufności, integralności lub dostępności danych, ze szczególnym uwzględnieniem możliwości naruszenia praw lub wolności osób fizycznych.

Jednocześnie można wyodrębnić kilka celów realizacji analizy ryzyka w bibliotece. Są to jednocześnie korzyści wynikające z takiego działania. Wśród nich priorytetowe znaczenie ma:

- wywiązanie się z obowiązku prawnego usankcjonowanego w art. 32 ust. 2 RODO (w przypadku kontroli przeprowadzonej przez Prezesa UODO, sytuacji spornej lub groźby nałożenia karty, w bibliotece będą się znajdowały udokumentowane dowody realizacji przepisów RODO w postaci dokumentacji analizy ryzyka),
- realne zmniejszenie ryzyka naruszenia poufności, integralności lub dostępności danych osobowych, czego konsekwencją jest zmniejszenie ryzyka braku realizacji lub naruszenia praw lub wolności osób fizycznych,
- przegląd obszarów deficytowych i słabych stron funkcjonowania biblioteki w zakresie ochrony danych osobowych oraz uświadomienie kadry kierowniczej i pracowników biblioteki w tym zakresie.

8.2. Metody analizy ryzyka.

I. Specyfika poszczególnych metod.

W przepisach RODO został wskazany obligatoryjny charakter opierania systemu ochrony danych osobowych w bibliotece na analizie ryzyka. Nie wskazano jednak konkretnej metodyki działania.

Oznacza to, że w poszczególnych bibliotekach analiza ryzyka może być przeprowadzana różnymi metodami i nie będzie to jednoznaczne z tym, że nie jest realizowana w sposób prawidłowy. Co więcej, w przepisach RODO nie wskazano obligatoryjnego zastosowania formy pisemnej analizy ryzyka. Teoretycznie ADO może więc wykazać, że przeprowadza analizę ryzyka w inny sposób i nie musi posiadać oraz udostępniać (w przypadku kontroli) plików w systemie informatycznym lub wydruków z przeprowadzonej analizy. W praktyce jednak udowodnienie realizacji analizy ryzyka w innej formie niż pisemna jest bardzo trudne, bądź też niemożliwe. Stąd rekomendowanym działaniem jest zbieranie dowodów na realizację tego procesu w formie pisemnej (elektronicznej lub papierowej).

Dyrekcja biblioteki musi podjąć decyzję odnośnie doboru metod analizy ryzyka. Przy jej podejmowaniu warto uwzględnić opinię IOD, jako specjalisty w zakresie ochrony danych osobowych znającego specyfikę funkcjonowania biblioteki. Możliwe jest kilka rozwiązań w tym zakresie:

- wdrożenie normy ISO/IEC 27005:2018 zawierającej zbiór wskazówek i wytycznych w zakresie efektywnego zarządzania ryzykiem,
- zastosowanie rozwiązań zaproponowanych przez pracowników Urzędu Ochrony Danych Osobowych w dwóch poradnikach. pt. „Jak rozumieć podejście oparte na ryzyku?[6]" oraz „Jak stosować podejście oparte na ryzyku?[7]",
- zastosowanie rozwiązań zaproponowanych przez redaktorów Kodeksu (zostały opisane w II części podrozdziału 8.2.),
- stworzenie własnej metody analizy ryzyka.

Zastosowanie normy ISO/IEC 27005:2018 ma niewątpliwie kilka istotnych mocnych stron. Jest to norma należąca do zbioru norm ISO/IEC 27000 odnoszących się do systemu zarządzania bezpieczeństwem informacji. Jak wskazano w podrozdziale 6.5. niniejszego Kodeksu, na zawartości merytorycznej normy opierają się niektóre przepisy RODO. Wadą takiego rozwiązania jest bez wątpienia konieczność posiadania fachowej wiedzy. Są to działania o profesjonalnym i specjalistycznym charakterze. Dodatkowo zakup normy wymaga zaangażowania dodatkowych środków finansowych.

Zastosowanie rozwiązań, które opisano w poradnikach przygotowanych przez pracowników Urzędu Ochrony Danych Osobowych również będzie ściśle związane z realizacją przepisów RODO, ponieważ podobnie jak rozporządzenie zostały one oparte na normach ze zbioru ISO/IEC 27000. W przeciwieństwie do zastosowania pierwotnej normy takie rozwiązanie jest bezpłatne, ponieważ treść poradników dostępna jest na stronach internetowych Prezesa UODO. W tym przypadku słabą stroną rozwiązania ponownie jest konieczność posiadania specjalistycznej wiedzy. Szczegółowy opis metodyki analizy ryzyka zawarty w drugiej części poradnika jest bowiem skomplikowany, a przedstawione metody będą trudne do zastosowania przez osoby nieposiadające dużego doświadczenia w zarządzaniu ryzykiem.

Zasadniczą zaletą zastosowania rozwiązań zaproponowanych przez redaktorów Kodeksu (ich opis znajduje się w drugiej części rozdziału 8.2.) jest ich przystępny charakter i możliwość zastosowania również przez ADO, którzy nie mają doświadczenia w zarządzaniu ryzykiem. Ponadto, zaproponowane rozwiązania charakteryzują się szerokim potencjałem implementacyjnym niezależnie od specyfiki funkcjonowania biblioteki, w której mogą zostać zastosowane. Sprawdziły się w praktyce w podmiotach, w których zostały wdrożone. Słabą stroną rozwiązania jest konieczność subiektywnego wyboru procesów przetwarzania w zbiorach danych (przeprowadzenie analizy wszystkich proce-

[6] A. Kaczmarek, M. Młotkiewicz, A. Łapińska, A. Miłocha, M. Mazur, *Jak rozumieć podejście oparte na ryzyku? Poradnik RODO. Podejście oparte na ryzyku. Część 1*, https://uodo.gov.pl/data/filemanager_pl/706.pdf [dostęp 31.08.2019].

[7] A. Kaczmarek, M. Młotkiewicz, A. Łapińska, A. Miłocha, M. Mazur, *Jak stosować podejście oparte na ryzyku? Poradnik RODO. Podejście oparte na ryzyku. Część 2*, https://uodo.gov.pl/data/filemanager_pl/707.pdf [dostęp 31.08.2019].

sów byłoby niewspółmiernie czasochłonne). Adekwatny wybór w tym zakresie może wymagać kilku prób, bez wątpienia nie zawsze udaje się za pierwszym razem.

W bibliotekach można też zastosować inne metody analizy ryzyka. Mogą być inspirowane wskazanymi normami, poradnikami i propozycjami, ale też opracowane na podstawie innych źródeł, bądź też pozytywnych doświadczeń np. z analizowaniem ryzyka w ramach kontroli zarządczej. Najważniejsze jest to, żeby analiza ryzyka była dostosowana do wieloaspektowej specyfiki działalności biblioteki i umożliwiała późniejsze wykazanie wdrożenia przepisów RODO w praktyce.

II. Metoda rekomendowana przez redaktorów Kodeksu.

Efektywne przeprowadzanie analizy ryzyka wiąże się z koniecznością stworzenia precyzyjnej instrukcji wewnętrznej w zakresie tego działania. W przypadku jakichkolwiek wątpliwości pracownicy biblioteki analizujący ryzyko mają się wówczas do czego odnieść. Ułatwia to też zapewnienie ciągłości analizy, jeżeli dochodzi do zmian kadrowych lub zmian zakresu obowiązków pracowników. Dlatego całe opracowanie analizy ryzyka warto podzielić na dwie części:

1. Część teoretyczną (opisową) analizy ryzyka.
2. Część analityczną analizy ryzyka.

Część teoretyczna powinna stanowić element analizy ryzyka, który tylko sporadycznie jest poddawany modyfikacjom. Szczególnie istotne jest, aby przygotować ją starannie i w odniesieniu do rzeczywistych zasobów biblioteki. Ten element opracowania powinien dostarczać jak najwięcej wartościowych informacji osobom, które przystępują do wykonania analizy ryzyka. Część teoretyczna w szczególności powinna zawierać:

a) Wskazanie celu i podstawy prawnej analizy ryzyka.

Podstawą prawną analizy ryzyka jest art. 32 ust. 2 RODO. Celem jest m.in. prewencja zagrożeń bezpieczeństwa informacji. Podstawa prawna i cele analizy ryzyka zostały szczegółowo omówione w podrozdziale 8.1 niniejszego Kodeksu.

b) Identyfikację i ocenę zasobów chronionych.

Zgodnie z rekomendacjami zawartymi w poradniku napisanym przez pracowników Urzędu Ochrony Danych Osobowych podczas identyfikacji zasobów warto wziąć pod uwagę aktywa. Zgodnie z normą PN-ISO/IES 27005 aktywa dzielą się na podstawowe (np. procesy, informacje) oraz wspierające (np. sprzęt, oprogramowanie, siedziba, struktura organizacyjna). Zasoby chronione można także podzielić na:

- informacje chronione (np. dane osobowe, System Zarządzania Bezpieczeństwem Informacji),
- procesy przetwarzania informacji (np. gromadzenie, edytowanie, kopiowanie, udostępnianie, niszczenie),
- sprzęt (np. serwery, komputery stacjonarne, drukarki, niszczarki),
- oprogramowanie (np. programy antywirusowe, zapory systemowe),
- obszary przetwarzania informacji (np. obszary podwyższonego ryzyka),
- osoby (np. osoby, których dane dotyczą, osoby upoważnione do przetwarzania danych osobowych),
- infrastrukturę sieciową (np. zapewnienie zasilania sprzętu, zarządzanie serwerami),
- strukturę organizacyjną ADO (np. osoby odpowiedzialne za nadzór nad przetwarzaniem danych zgodnie z przepisami prawa, osoby odpowiedzialne za nadzór nad uprawnieniami użytkowników),

c) Identyfikację procesów przetwarzania danych osobowych w ramach zasobów chronionych, w stosunku do których należy przeprowadzić analizę ryzyka.

Proponowana metoda analizy ryzyka opiera się na analizie poszczególnych zbiorów danych osobowych. W każdym zbiorze należy zidentyfikować procesy przetwarzania danych osobowych w ramach zasobów chronionych, w stosunku do których należy przeprowadzić analizę ryzyka. Najlepiej jest wybrać kilka procesów w ramach każdego zbioru, które będą miały istotne znaczenie z punktu widzenia realizacji zadań przez bibliotekę. Przykładowe procesy przetwarzania w zbiorach danych osobowych to:

- gromadzenie danych,
- przechowywanie danych,
- prowadzenie korespondencji mailowej,
- drukowanie i kopiowanie danych,
- przetwarzanie danych przy użyciu urządzeń mobilnych/ponownym wykorzystaniu nośników informacji,
- przenoszenie danych (przez osobę, której dane dotyczą),
- usuwanie danych,
- udostępnianie danych na żądanie,
- niszczenie danych,
- interpretowanie danych.

Jako przykład identyfikacji procesów można wskazać takie działanie na przykładzie danych subskrybentów newsletteru. Mogą to być np. następujące procesy przetwarzania w zbiorach danych:

gromadzenie danych odbiorców newsletteru,

- wysyłanie newsletteru,
- przechowywanie danych subskrybentów,
- usuwanie danych subskrybentów,
- powierzenie danych subskrybentów.

Innym przykładem może być identyfikacja procesów w zbiorze danych pracowników zatrudnionych na umowę o pracę. Mogą to być np.:

- gromadzenie danych pracowników zatrudnionych na umowę o pracę,
- powierzenie danych pracowników zatrudnionych na umowę o pracę,
- udostępnianie danych pracowników zatrudnionych na umowę o pracę,
- usuwanie danych pracowników zatrudnionych na umowę o pracę.

d) Identyfikacja zagrożeń.

Bazując na klasyfikacji zagrożeń zaproponowanej przez twórców zbioru norm ISO/IEC 27000 odnoszących się do systemu zarządzania bezpieczeństwem informacji, zagrożenia można podzielić na:

- ryzyka dla bezpieczeństwa teleinformatycznego (np. utrata danych, awaria sprzętu, błędna konfiguracja, nieaktualne oprogramowanie),
- ryzyka dla bezpieczeństwa fizycznego (np. brak niszczarek, klęski żywiołowe, niewłaściwa kontrola dostępu),
- ryzyka dla bezpieczeństwa prawnego (np. niewłaściwa kontrola zapisów umownych, niewłaściwe realizowanie obowiązków informacyjnych),
- ryzyka dla bezpieczeństwa organizacyjno-osobowego (np. niefrasobliwe rozmowy, kradzież dokumentów, kradzież sprzętu komputerowego).

Przedstawiony podział jest tylko jedną z propozycji identyfikowania zagrożeń. ADO w porozumieniu z IOD powinien dokonać klasyfikacji ryzyk w oparciu o codzienne problemy w funkcjonowaniu biblioteki.

e) Opis zasad i kryteriów analizy ryzyka.

Proponowana metoda analizy ryzyka zakłada jej przeprowadzanie w oparciu o 6 zasad dotyczących przetwarzania danych osobowych określonych w art. 5 ust. 1 RODO:

- zgodność z prawem, rzetelność i przejrzystość
- ograniczenie celu
- minimalizacja danych
- prawidłowość
- ograniczenie przechowywania
- integralność i poufność.

W części teoretycznej (opisowej) analizy ryzyka w bibliotece warto zamieścić całą treść art. 5 ust. 1 RODO, żeby uniknąć ewentualnych błędów interpretacyjnych w zakresie poszczególnych zasad. Następnie dla każdego z wybranych procesów przetwarzania w zbiorze danych należy oszacować prawdopodobieństwo wystąpienia ryzyka używając 3-stopniowej skali, w której:

- 1 oznacza ryzyko niskie lub brak ryzyka (nie dotyczy),
- 2 oznacza ryzyko średnie,
- 3 oznacza ryzyko wysokie.

Decyzję o tym jakie jest prawdopodobieństwo wystąpienia ryzyka dla konkretnego procesu w zbiorze danych należy podjąć na podstawie z góry przyjętych kryteriów. Jeżeli suma poszczególnych wartości dla wszystkich sześciu badanych parametrów wynosi:

- od 6 do 9, oznacza to ryzyko niskie,
- od 10 do 13, oznacza to ryzyko średnie,
- od 14 do 18, oznacza to ryzyko wysokie.

Efektywne przeprowadzenie analizy możliwe jest z wykorzystaniem tabeli nr 1, która została zamieszczona w podrozdziale 8.4 niniejszego Kodeksu.

Jednocześnie warto z góry określić cztery możliwe formy postępowania z ryzykiem:

- akceptację ryzyka – świadoma decyzja o niewprowadzaniu żadnych zmian,
- redukcję ryzyka – polega na obniżeniu poziomu ryzyka poprzez zmianę prawdopodobieństwa wystąpienia określonego zdarzenia lub zmniejszenie skutków jego wystąpienia,
- unikanie ryzyka – unikanie działań, które powodują ryzyka (np. jeżeli koszt redukcji jest zbyt wysoki),
- przeniesienie ryzyka – polega np. na wykupieniu ubezpieczenia.

Warto przyjąć, że akceptacja ryzyka jest możliwa tylko w przypadku zdiagnozowania ryzyka niskiego. Natomiast w przypadku ryzyka średniego lub wysokiego konieczne jest wskazanie planu naprawczego lub zaleceń minimalizujących ryzyko. Jednocześnie wysokie ryzyko wiąże się z koniecznością przeprowadzenia oceny skutków dla ochrony danych.

Część analityczna analizy ryzyka będzie natomiast stanowiła realizację założeń części teoretycznej (opisowej) w praktyce. Dla każdego zbioru danych należy sporządzić odrębną tabelę i oszacować ryzyko dla wybranych procesów przetwarzania w danym zbiorze. Oczywiście należy podjąć także ewentualne dalsze kroki, jeżeli ryzyko jest średnie lub wysokie. Analiza ryzyka nie musi być przeprowadzana jednocześnie we wszystkich zbiorach. Można sukcesywnie analizować ryzyko w pojedynczych zbiorach. Autonomiczną decyzją ADO jest określenie częstotliwości przeprowadza-

nia analizy ryzyka. Biorąc pod uwagę specyfikę funkcjonowania bibliotek warto zarekomendować, żeby analiza była dokonywana co najmniej raz w roku odnośnie każdego zbioru danych.

8.3. Ocena skutków dla ochrony danych.

Ocena skutków dla ochrony danych (w literaturze przedmiotu i poradnikach często określana jako „DPIA", ze względu na nazwę w języku angielskim - Data Protection Impact Assessment) to działanie precyzyjnie opisane w art. 35 RODO. W przypadku oceny skutków ADO nie musi sięgać po poradniki lub normy i wybierać adekwatnej metody, ponieważ instrukcja dotycząca poszczególnych etapów działania znajduje się w przepisach RODO. Pracownicy UODO zakwalifikowali ocenę skutków jako ostatni element analizy ryzyka (w poradnikach wskazanych w podrozdziale 8.2. niniejszego Kodeksu). Bez wątpienia działanie to jest ściśle związane z podejściem do ochrony danych osobowych opartym na analizie ryzyka. Warto jednak podkreślić, że nie do każdej analizy ryzyka należy przeprowadzić ocenę skutków, a z drugiej strony w niektórych sytuacjach będzie ona miała charakter obligatoryjny niezależnie od tego jaki poziom ryzyka ustali ADO.

Poprawne zrozumienie istoty oceny skutków wymaga zapoznania się z preambułą RODO. W kilku motywach preambuły wyjaśniono, jakie były intencje usankcjonowania tego działania w przepisach RODO. W motywie 84. jako cel oceny skutków wskazano poprawienie przestrzegania przepisów RODO, gdy „operacje przetwarzania mogą wiązać się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych". Poinformowano także, że „należy zobowiązać administratora do dokonania oceny skutków dla ochrony danych w celu oszacowania w szczególności źródła, charakteru, specyfiki i powagi tego ryzyka". Jednocześnie wskazano, że „wyniki oceny należy uwzględnić przy określaniu odpowiednich środków" (które należy zastosować, by wykazać, że przetwarzanie danych osobowych odbywa się zgodnie z RODO). Natomiast w motywie 89. przypomniano, że przed wejściem w życie RODO, każdy ADO miał obowiązek zawiadamiania organów nadzorczych o przetwarzaniu danych osobowych. W Polsce miało to formę zgłaszania danych osobowych do GIODO, a w przypadku zbiorów danych wrażliwych, uzyskiwania uprzedniej zgody organu na przetwarzanie. Likwidując ten obowiązek, twórcy nowych uregulowań prawnych zdecydowali o zastąpieniu go „skutecznymi procedurami i mechanizmami koncentrującymi się w zamian na tych rodzajach operacji przetwarzania, które ze względu na swój charakter, zakres, kontekst i cele mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych". Oznacza to, że głównym celem oceny skutków dla ochrony danych jest, podobnie jak w przypadku analizy ryzyka, zwiększenie bezpieczeństwa przetwarzania danych osobowych, ze szczególnym uwzględnieniem prewencji zagrożeń naruszenia lub braku realizacji praw lub wolności osób fizycznych.

Przed analizą poszczególnych etapów oceny skutków dla ochrony danych warto zwrócić uwagę, iż samo istnienie wymogu prawnego w tym zakresie potwierdza zasadność przeprowadzania analizy ryzyka w formie pisemnej (elektronicznej lub papierowej). Wynika to z faktu, iż zgodnie z art. 35 ust. 1 RODO „jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych". Dyrekcja biblioteki musi zatem z jednej strony wykazać przyczyny przeprowadzenia oceny skutków w niektórych przypadkach, z drugiej przedstawić rzetelne powody uzasadniające brak przeprowadzenia oceny skutków w innych przypadkach.

W praktyce ocenę skutków należy przeprowadzić w dwóch przypadkach. Pierwszy z nich dotyczy sytuacji, w której z analizy ryzyka (niezależnie od wybranej metodyki jej przeprowadzania)

wynika, iż istnieje wysokie ryzyko naruszenia praw lub wolności osób fizycznych. W praktyce będzie to oznaczało, że w każdym przypadku, w którym w przeprowadzonej analizie pojawi się wysokie ryzyko, konieczne będzie przeprowadzenie takiej oceny. Jest bowiem bardzo mało prawdopodobne, że wskazanie na wysokie ryzyko w przypadku analizy ryzyka dotyczącej ochrony danych osobowych nie będzie implikowało wysokiego ryzyka naruszenia praw lub wolności osób fizycznych. Drugi przypadek, w którym przeprowadzenie oceny skutków ma charakter obligatoryjny to takie przetwarzanie danych osobowych w bibliotece, które można zakwalifikować jako jeden z elementów wykazu rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych, ustanowionego i podanego do publicznej wiadomości przez Prezesa Urzędu Ochrony Danych Osobowych. Aktualny wykaz został opublikowany w Monitorze Polskim w formie Komunikatu[8] 8 lipca 2019 r. Warto jednak regularnie sprawdzać status Komunikatu w Internetowym Systemie Aktów Prawnych, ponieważ może zostać zaktualizowany. Jednocześnie istnieje możliwość ustanowienia i podania do publicznej wiadomości przez organ nadzorczy wykazu rodzajów operacji przetwarzania niepodlegających wymogowi dokonania oceny skutków dla ochrony danych. Pojawianie się takiego wykazu oznaczałoby najprawdopodobniej, iż nawet jeśli podczas analizy ryzyka wskazano wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w niektórych przypadkach nie będzie konieczne przeprowadzenie oceny skutków. Biorąc pod uwagę obecny stan prawny warto podkreślić, iż taki wykaz nie powstał. Jednak nawet jeśli powstanie, warto zarekomendować przeprowadzenie oceny skutków na potrzeby ADO nawet jeśli będzie miała ona charakter fakultatywny. Jej przeprowadzenie nie jest skomplikowanym działaniem, a pozwala na lepszą ocenę potencjalnych zagrożeń bezpieczeństwa danych osobowych w bibliotece.

Jeżeli okaże się, że przetwarzanie danych osobowych w bibliotece wiąże się ze spełnieniem jednej z dwóch powyższych przesłanek, należy przystąpić do oceny skutków dla ochrony danych. Wówczas ADO musi poddać refleksji operacje przetwarzania wymagające oceny skutków, poprzez analizę celu, konieczności takiego działania, ryzyka z nim związanego oraz powodów takiego ryzyka. Ocena skutków polega na wypełnieniu kwestionariusza składającego się z (co najmniej) 4 elementów wskazanych w art. 35 ust. 7 RODO. Powinny one zawierać:

- systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora,
- ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów,
- ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą,
- środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

Wymóg prawny usankcjonowany w art. 35 RODO musi być rozpatrywany łącznie z art. 36 rozporządzenia. Zgodnie z nim „jeżeli ocena skutków dla ochrony danych, o której mowa w art. 35, wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania administrator konsultuje się z organem nadzorczym". Oznacza to konieczność konsultowania z Prezesem UODO najbardziej problematycznych operacji przetwarzania, co do których dyrekcja biblioteki nie widzi możliwości zminimalizowania ryzyka na własną rękę. Ponadto, w art. 36 RODO wskazano zasady konsultacji z organem nadzorczym i zakres czasowy poszczególnych działań.

[8] Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (M.P. 2019 poz. 666).

Warto zwrócić uwagę, iż w przepisach RODO podkreślono szczególną rolę IOD w ocenie skutków dla ochrony danych. Z jednej strony w art. 35 ust. 3 wskazano, iż „dokonując oceny skutków dla ochrony danych, administrator konsultuje się z inspektorem ochrony danych, jeżeli został on wyznaczony". Z drugiej, wśród zadań IOD (art. 39 RODO) wskazano „udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35". Do przeprowadzenia oceny skutków dyrekcja biblioteki powinna też zaangażować innych pracowników, szczególnie jako konsultantów w zakresie obszarów, w których się specjalizują. Prawidłowo wykonana ocena powinna być bowiem rzetelną analizą sytuacji, która może realnie przyczynić się do zwiększenia bezpieczeństwa przetwarzania danych osobowych.

8.4. Dobre praktyki, wytyczne i wskazówki.

Tabela nr 1. Szablon analizy ryzyka dla jednego procesu przetwarzania w zbiorze.

Ryzyko wystąpienia dla poszczególnych procesów. Skala: 1 – Niskie lub nie dotyczy, 2 – Średnie, 3 –Wysokie	
Rozliczalność, rzetelność i przejrzystość	
Ograniczenie celu	
Minimalizacja danych	
Prawidłowość i aktualność danych	
Ograniczenie przechowywania	
Integralność i poufność	
Zidentyfikowane ryzyko dla zasobu, według skali Niskie ryzyko: 6-9, Średnie ryzyko: 10-13, Wysokie ryzyko 14-18	
Postępowanie z ryzykiem /decyzja	
Uzasadnienie akceptacji wyliczonego poziomu ryzyka	
Plan naprawczy/zalecenia minimalizujące ryzyko	

Tabela nr 2. Ocena skutków dla ochrony danych.

PRZEDMIOT OCENY	
Systematyczny opis planowanych operacji przetwarzania i celów przetwarzania (gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora).	
Ocena (wraz z uzasadnieniem) – czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów?	
Ocena (wraz z uzasadnieniem) ryzyka naruszenia praw lub wolności osób, których dane dotyczą.	
Środki planowane w celu zaradzenia ryzyku*.	
Wnioski i decyzja (ostateczna ocena skutków).	

* W tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

9 SZCZEGÓLNE ASPEKTY PRZETWARZANIA DANYCH OSOBOWYCH PRZEZ BIBLIOTEKI

9.1. Strona internetowa biblioteki.

Strona internetowa biblioteki służy do komunikacji z użytkownikami, w szczególności, aby poinformować o godzinach otwarcia, zasadach korzystania z ich oferty, wydarzeniach, ale także aby promować swoją działalność i cele statutowe. Strona to także narzędzie umożliwiające korzystanie z usług bibliotecznych za pośrednictwem OPAC. W związku ze świadczonymi usługami na stronie internetowej powinny zostać zamieszczone:

1. Regulaminy korzystania z biblioteki oraz usług bibliotecznych.
2. Regulamin wydarzeń/imprez.
3. Regulamin korzystania z usługi OPAC (zgodny z wymaganiami art. 8 UŚUDE.
4. Klauzula informacyjna dla osób korzystających z usług bibliotecznych.
5. Klauzula informacyjna dotycząca monitoringu wizyjnego (jeżeli jest wykorzystywany).
6. Dane rejestrowe biblioteki (np. w zakładce kontakt i/lub w BIP).

Szczególnie istotne jest uwzględnienie zasad korzystania z OPAC przez użytkowników, ponieważ jest to słabość wielu regulaminów bibliotecznych, które w swojej treści w ogóle nie odnoszą się do tej usługi. Obowiązki informacyjne wobec osób, których dane przetwarzane są w ramach działalności bibliotecznej, zwykło się realizować poprzez zamieszczenie niezbędnej klauzuli w regulaminie danej usługi. Nic nie stoi jednak na przeszkodzie, aby na stronie internetowej biblioteki zamieścić komplet obowiązków informacyjnych, tzn. skierowany do czytelników, uczestników wydarzeń, osób kontaktujących się z biblioteką, osób niezarejestrowanych korzystających z innych usług, przetwarzanych w związku z monitoringiem wizyjnym, ale także pracowników, zleceniobiorców, kandydatów do pracy lub kontrahentów. W ten sposób każda z tych osób, będzie mogła zapoznać się z niezbędnymi informacjami w dowolnym momencie. Takie klauzule można zamieścić w zakładce „kontakt" lub w BIP biblioteki.

I. Zabezpieczenie strony.

Strona internetowa biblioteki jest także narzędziem służącym do przetwarzania danych osobowych, w szczególności czytelników korzystających z OPAC, ale także osób, które pozostawiają swoje dane za pośrednictwem formularza kontaktowego. Obowiązkiem administratora danych jest należyte zabezpieczenie gromadzonych danych, w szczególności poprzez zapewnienie zabezpieczenia strony internetowej poprzez certyfikat SSL. To, że strona posiada stosowany certyfikat, można rozpoznać

po adresie, rozpoczynającym się od „http**s**", oraz symbolem zamkniętej kłódki przy tym adresie. Certyfikat SSL zapewnia szyfrowanie danych przesyłanych za pośrednictwem strony internetowej, takich jak dane do logowania do OPAC, dane do logowania do strony CMS, czy dane przekazywane przez formularze kontaktowe lub zapisu na zajęcia. Warto zwrócić uwagę także na to, że nawet jeżeli na stronie internetowej nie udostępniono żadnych usług dla użytkowników, to samo zebezpieczenie dostępu do CMS strony jest już wystarczającym argumentem, do zakupu niezbędnego oprogramowania. Niezabezpieczenie strony daje możliwość zainfekowania jej i na przykład wykorzystanie do rozsyłania wirusów na urządzenia osób, które odwiedzą stronę. Brak certyfikatu SSL istotnie wpływa także na obniżenie tzw. ratingu strony, czyli jej pozycję w wynikach wyszukiwania. Niektóre przeglądarki uniemożliwiają lub utrudniają odwiedzenie takiej strony, co jest dodatkowym argumentem za zakupem certyfikatu. Warto podkreślić, że na rynku są dostępne także bezpłatne certyfikaty, jednak korzystanie z nich wymaga dość częstego odnawiania, a więc korzystania ze wsparcia informatyka i pamiętania o odnawianiu.

Poza zabezpieczeniem przesyłanych danych, należy zwrócić uwagę na zainstalowane kody, cookies i wtyczki. Podstawowa zasada jest taka, że im mniej tego typu rozwiązań jest stosowanych, tym lepiej. Bardzo popularne w ostatnim czasie jest domyślne instalowanie na stronie internetowej kodów śledzących należących do Google i Facebook. Najczęściej osoby, które dokonują tych czynności technicznych, nie zdają sobie sprawy z konsekwencji. Dla przykładu Google Analitics [GA], który pozwala śledzić statystyki odwiedzin, jest jedną z najczęściej wykorzystywanych tego typu usług. Podmiot instalujący kody GA na swojej stronie internetowej, otrzymuje bezosobowe dane, które nie umożliwiają identyfikacji użytkowników. Jednocześnie Google Lcc otrzymuje za pośrednictwem zainstalowanych kodów informacje, które nie tylko pozwalają zidentyfikować użytkownika, ale także wyświetlać mu określone treści reklamowe (określać co robi, co lubi, gdzie jest, jakie informacje mu wyświetlić). Korzystanie z tej usługi jest bezpłatne pod warunkiem, że administrator strony, uzyska zgodę na przetwarzanie danych osobowych za pośrednictwem tego narzędzia (oraz innych narzędzi monitorujących aktywność, w tym cookies), a także udostępnieni w swojej polityce prywatności link do regulaminu usługi GA. Zgodnie z regulaminem usługi, Google jest uprawniony w dowolnym momencie zweryfikować, czy administrator dopełnił formalności, a także zażądać od niego dowodów w tym zakresie. Jeszcze bardziej rygorystyczne jest korzystanie z narzędzi dostarczanych przez Facebook Inc, takich jak niewzbudzający podejrzeń Pixel lub Widget. Są to narzędzia, które śledzą każdego użytkownika, nawet takiego, który nie jest zalogowany do Facebooka lub nie korzysta z jego usług. Co więcej, podmiot, który korzysta z tych narzędzi staje się współadministratorem danych osobowych przetwarzanych przez Facebook, co w konsekwencji może mieć wpływ na zakres jego odpowiedzialności. Warto zwrócić uwagę na to, że regulamin Facebooka jest jednostronny i albo klient go akceptuje albo nie, nie ma w tym przypadku możliwości negocjacji. W praktyce dane pozyskane przez niewzbudzającą podejrzeń grafikę (Pixel Facebook) umożliwiają portalowi Facebook dostarczanie treści reklamowych swoich klientów na podstawie decyzji użytkownika. Warto zwrócić uwagę, że o ile usługa GA daje potencjalne korzyści bibliotece, to usługi Facebooka nie przynoszą żadnych korzyści, poza tym, że to „ładnie" lub „nowocześnie" wygląda. Ponownie biblioteka jest zobligowana do pozyskania zgody na wykorzystanie takiego narzędzia, (uwzględniając, że zgoda będzie dotyczyła także udostępnienienia na rzecz Facebooka i jego partnerów), a także udostępnienia użytkownikom regulaminu usług Facebook. W związku z powyższymi zalecane jest zastąpienie usługi GA, zwykłymi statystykami dostarczanymi przez CMS (o ile faktycznie jest to niezbędne). Taka usługa powinna być tak spersonalizowana, aby gromadzić tylko niezbędne informacje (liczba wejść,

czas spędzony na stronie), bez adresów IP, czy danych o urządzeniu użytkownika. W miejsce Pixela Facebooka można zastosować zwykłą grafikę, która wygląda tak samo i po kliknięciu przeniesienia na fanpage biblioteki, ale nie zbiera danych o użytkowników. Podobnie w miejsce Widgetu, który pojawia się z boku, zasłaniając treści, można zastosować estetycznie zrobioną grafikę, zachęcającą do odwiedzenia profilu w mediach społecznościowych.

II. Polityka prywatności i cookies.

Przyjętą zasadą jest zamieszczenie na stronie internetowej polityki prywatności i cookies, w której zamieszcza się obowiązek informacyjny z art. 13 ust. 1 i 2 RODO. Jeżeli są wykorzystywane na stronie zewnętrzne usługi, wówczas należy opisać zasady przetwarzania danych poprzez te usługi. Kiedyś większość z usług wykorzystywała cookies, ale obecnie coraz częściej są to po prostu kody śledzące, które zostały dodane do kodu źródłowego strony internetowej, czyli śledzą użytkownika na podobnej zasadzie jak cookies, pomimo że nie są to cookies. Informacje o zasadach działania usługi zawsze udostępnia producent tej usługi w swoim regulaminie, najczęściej z zaznaczeniem, jakie informacje należy wprowadzić do polityki prywatności na swojej stronie, jeżeli zamierza się wykorzystać konkretne narzędzie.

Polityka prywatności powinna określać kto jest administratorem strony, jakie dane są gromadzone poprzez stroną za pośrednictwem poszczególnych usług, do jakich celów te dane są wykorzystywane, klauzulę informacyjną z RODO, a także kontakt do administratora. W przypadku korzystania z usług, które wymagają zgody użytkownika (czyli gromadzenie jego danych przez cookies i inne kody śledzące), przed wejściem na stronę użytkownik powinien zostać poproszony o wyraźnie zgody na przetwarzanie danych i mieć możliwość zapoznania się z polityką prywatności biblioteki. Nie wyrażenie zgody powinno sprawić, że mechanizmy służące do śledzenia użytkownika będą wyłączone. W praktyce korzystanie z takch mechanizmów oznacza dodatkowy koszt właściwego oprogramowania strony internetowej.

III. Media społecznościowe.

Warto wspomnieć, że prowadzenie fanpage na Facebooku także wiąże się z obowiązkami wynikającymi z przepisów o ochronie danych osobowych. Przede wszystkim biblioteka, jako właściciel fanpage prowadzonego w ramach Facebooka, jest administratorem danych przetwarzanych w ramach tego fanpage. W przeszłości panowało przekonanie, że administratorem danych jest Facebook, jednakże obecnie nie ma wątpliwości, że to administrator Fanpage decyduje o celach i środkach przetwarzanych danych. Potwierdza to także orzecznictwo Trybunału Sprawiedliwości UE[9]. Odpowiednie postanowienia dotyczące odpowiedzialności administratora fanpage zostały także określone w regulaminie Facebooka. W związku z korzytaniem z tego szczególnego narzędzia do promowania swoich usług, należy wypełnić obowiązki informacyjne wobec użytkowników. Najłatwiej zrealizować to poprzez dodanie odpowiednich zapisów do polityki prywatności na stronie internetowej biblioteki, a następnie udostępnienie adresu strony na fanpge, w części „Informacje". Facebook udostępnił tam możliwość wskazania adresu polityki prywatności administratora fanpage. Niewypełnienie obowiązków informacyjnych wobec użytkowników fanpage jest naruszeniem przepisów RODO.

[9] Wyrok w sprawie C-210/16 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein / Wirtschaftsakademie Schleswig-Holstein GmbH

9.2. Organizowanie konkursów.

Rolą bibliotek jako instytucji kultury jest podejmowanie szeroko pojętych działań mających na celu promowanie czytelnictwa. Wśród takich aktywności można wyróżnić kupowanie nowości, wspieranie bibliotek szkolnych poprzez zapewnianie lektur, lekcje biblioteczne, spotkania autorskie, organizowanie wydarzeń kulturalnych, a także organizowanie konkursów. Celem konkursu jest aktywizacja czytelników, ale także zachęcenie innych osób do wizyty w bibliotece i skorzystanie z jej oferty. Należy także podkreślić, że skutecznie zaplanowany i przeprowadzony konkurs buduje pozytywny wizerunek marki biblioteki oraz zachęca do jej odwiedzenia. Prace konkursowe, jako dzieła o szczególnych walorach artystycznych lub hasła promocyjne, także wpływają na promowanie wizerunku biblioteki oraz samego czytelnictwa.

I. Konkurs a gra losowa.

Na wstępie warto podkreślić, że prowadzenie działalności promocyjnej poprzez organizowanie konkursów lub gier losowych, wiąże się z konkretnymi obowiązkami określonymi w przepisach powszechnie obowiązującego prawa, w szczególności na organizatorze takiej akcji ciążą obowiązki podatkowe. Przez gry losowe należy rozumieć, takie gry, których wynik jest oparty na przypadku. Przykładami gier losowych organizowanych w bibliotekach będą, w szczególności (art. 2 ustawy o grach hazardowych):

a. gry liczbowe – gry, w których wygraną uzyskuje się przez prawidłowe wytypowanie liczb, znaków lub innych wyróżników, a wysokość wygranych zależy od łącznej kwoty wpłaconych stawek,
b. loterie pieniężne, w których uczestniczy się przez nabycie losu lub innego dowodu udziału w grze, a podmiot urządzający loterię oferuje wyłącznie wygrane pieniężne,
c. gry cylindryczne, w których uczestniczy się w grze przez wytypowanie liczb, znaków lub innych wyróżników, a wysokość wygranej zależy od określonego z góry stosunku wpłaty do wygranej, zaś wynik gry ustalany jest za pomocą urządzenia obrotowego lub gry cylindryczne urządzane na tych zasadach w sieci Internet,
d. gry w kości,
e. gry bingo fantowe, w której uczestniczy się przez nabycie przypadkowych zestawów liczb z ustalonego z góry zbioru liczb, a podmiot urządzający grę oferuje wyłącznie wygrane rzeczowe,
f. loterie fantowe, w których uczestniczy się przez nabycie losu lub innego dowodu udziału w grze, a podmiot urządzający loterię oferuje wyłącznie wygrane rzeczowe.

W każdej ze wskazanych gier, istotnym czynnikiem służącym do określenia zwycięzcy jest przypadek. Grą losową będzie także gra, w której wśród uczestników zostaną wylosowani zwycięzcy. Konkurs odróżnia od gry losowej konieczność wykazania się przez uczestnika umiejętnościami wskazanymi w zasadach konkursu, a także to, że nagrody są przyznawane najlepszym uczestników. Bardzo wiele konkursów dotyczy stworzenia autorskiego dzieła, w postaci zdjęcia, obrazu, rzeźby, wiersza, opowiadania, hasła reklamowego. Uczestnik konkursu rywalizuje z innymi uczestnikami, a jego zwycięstwie decydują obiektywne kryteria wyboru określone przez organizatora, a nie szczęście.

Organizowanie gier losowych, jak loterie fantowe czy bingo z nagrodami, jest oczywiście dopuszczalne i możliwe do realizacji w bibliotece, jednakże musi zostać zrealizowane zgodnie z wymogami ustawy o grach hazardowych, na podstawie otrzymanego zezwolenia lub zgłoszenia. Jeżeli wartość puli nagród w loterii fantowej lub bingo fantowym nie przekracza określonej w art. 70 ustawy o grach hazardowych „kwoty bazowej" wówczas, warunkiem zorganizowania gry jest zgłoszenie

jej co najmniej 30 dni przed planowaną datą rozpoczęcia do naczelnika urzędu celno-skarbowego, na którego obszarze właściwości miejscowej będzie przeprowadzana gra. Kwota bazowa dla danego roku kalendarzowego jest równa kwocie przeciętnego miesięcznego wynagrodzenia w sektorze przedsiębiorstw bez wypłat nagród z zysku, w drugim kwartale roku poprzedniego, ogłoszonego w obwieszczeniu Prezesa GUS. Należy pamiętać, że organizowanie gier losowych rodzi obowiązki podatkowe, których wysokość i zasady rozliczenia określa ustawa o grach hazardowych.

Podobnie w przypadku organizowania konkursu niezbędne jest odprowadzenie podatku, chyba że został spełniony jeden z określonych w przepisach podatkowych warunków, zwalniających z tego obowiązku[10], w szczególności wartość nagrody jest niewielka (nie przekracza 200 zł[11]). Na Organizatorze ciąży obowiązek wykazania, że przeprowadzany konkurs nie był grą losową, co realizuje się poprzez opracowanie i upublicznienie regulaminu konkursu, a także sporządzenie protokołu obrad jurorów z wyboru zwycięzców. Warto podkreślić, że organy podatkowe są uprawnione do badania okoliczności przeprowadzania konkursu i sposobu rozliczenia podatku, więc wskazane jest przechowywanie dokumentacji związanej z organizowanymi w bibliotece konkursami i grami losowymi przez okres 5 lat kalendarzowych, licząc od kolejnego roku po zakończeniu konkursu.

II. Procesowe podejście do przetwarzania danych w związku z organizowaniem konkursu.

Jak wskazano we wcześniejszej części, zorganizowanie i przeprowadzenie konkursu, już na etapie jego planowania, wiąże się z koniecznością ustalenia, sposobu wyłaniania zwycięzców i sposobu przeprowadzania działania. Uwzględniając wymagania przepisów RODO, organizator konkursu, przed rozpoczęciem przetwarzania danych w celach konkursowych powinien dokonać analizy przyszłego procesu, w celu analizy ryzyka oraz wdrożenia środków niezbędnych do zapewnienia właściwej ochrony danych. Każdy konkurs wiąże się z potencjalnymi ryzykami naruszenia praw i wolności osób, więc powinien być konsultowany z inspektorem ochrony danych w bibliotece.

Analiza procesu przeprowadzenia konkursu powinna w szczególności obejmować:

1. Ustalenie, czy planowane działanie na pewno będzie konkursem, tzn. czy wybór zwycięzców nie jest oparty o czynniki losowe.
2. Identyfikacja innych podmiotów uczestniczących w przeprowadzaniu konkursu, tzn. współorganizatorzy, sponsorzy, zlecający przeprowadzenie konkursu.
3. Zasady uczestnictwa (wiek uczestników, inne warunki brzegowe) i zakres zbieranych danych.
4. Zasady zgłaszania uczestnictwa i przyjmowania prac konkursowych, w tym czy będzie pośrednik przekazujący zgłoszenia, np. szkoła.
5. Zasady oceny prac konkursowych, a także kto będzie tego dokonywał, np. osoby spoza biblioteki i odpowiadał za spisanie protokołu.
6. Wartość nagród oraz obowiązki podatkowe.
7. Sposób realizowania praw osób, których dane dotyczą.
8. Czas i sposób przechowywania danych uczestników i zwycięzców.
9. Sposób wręczenia nagród.
10. Sposób wykorzystania prac konkursowych po zakończeniu konkursu w kontekście praw autorskich.

[10] Porównaj z podrozdziałem: 4.2 Podstawy prawne przetwarzania danych w bibliotece (Dorota Mika).

[11] Jako podstawę opodatkowania organizator musi liczyć sumę wartości wszystkich nagród uzyskanych przez jednego zwycięzcę w ciągu jednego roku kalendarzowego.

Przeprowadzanie konkursów jest dość skomplikowanym procesem, wymagającym szerokiej wiedzy od organizatora, a także podjęcia wielu działań przed ich zorganizowaniem. Ważnym elementem spinającym cały proces konkursowy jest regulamin konkursu, w którym organizator opisuje wszystkie zasady przeprowadzania konkursu, od organizatora, zasad udziału, zasad wyboru zwycięzców, przez wartość nagród i zasady rozliczenia lub zwolnienia z podatku, a także obowiązek informacyjny z art. 13 ust. 1 i 2 RODO i zasady zgłaszania reklamacji. Ze względu na zawiłości prawne, każdy konkurs przed jego ogłoszeniem, powinien zostać zaakceptowany przez inspektora ochrony danych, a także głównego księgowego biblioteki.

III. Legalność przetwarzania danych uczestników i zwycięzców.

Istnieje kilka sprzecznych stanowisk w zakresie przesłanki legalizującej przetwarzanie danych osobowych uczestników konkursu. W zależności od źródła wskazuje się: umowę zwartą z uczestnikiem (art. 6 ust. 1 lit. b RODO), prawnie usprawiedliwiony interes administratora (art. 6 ust. 1 lit. f RODO), lub zgodę uczestnika (art. 6 ust. 1 lit. a RODO). Przeważa stanowisko, że to właśnie zgoda jest właściwą podstawą prawną, co potwierdza także fakt, że w organizowanych przez siebie konkursach polski organ nadzorczy wskazuje zgodę, jako przesłankę legalizującą przetwarzanie danych. Zgodnie z art. 7 oraz motywem 32 RODO, administrator powinien uzyskać zgodę w taki sposób, aby móc wykazać, że była dobrowolna i świadoma, ale także posiadać fizyczny dowód zgody uczestnika. W związku z tym przyjętą praktyką jest przyjmowanie zgłoszeń konkursowych na piśmie lub poprzez formularze konkursowe, gdzie uczestnik musi samodzielnie zaznaczyć okna zgody. Dopuszczalne jest także przyjęcie, że samo przysłanie zgłoszenia stanowi wyrażenie zgody na przetwarzanie danych, jako świadome działanie wykonane przez uczestnika. Jest to powszechnie stosowane w przypadku konkursów organizowanych za pośrednictwem Facebooka. W takim wypadku organizator powinien wyraźnie określić w regulaminie konkursu, że zgłoszenie jest równoważne ze zgodą, zalecany jest także taki zapis na karcie zgłoszeniowej lub odpowiednio pod formularzem konkursowym na stronie internetowej, czy postem na konkursowym na Facebooku.

Odrębną kwestią jest nagradzanie najlepszych czytelników. Biorąc pod uwagę promocję czytelnictwa jako jeden z celów działalności bibliotek nagradzanie najlepszych czytelników (np. za liczbę przeczytanych książek lub aktywność w działalności bibliotecznych), można zakwalifikować, jako prawnie usprawiedliwiony interes administratora, podobnie jak wręczanie nagród dla najlepszych uczniów przez szkołę[12].

Należy zwrócić uwagę na to, że zgoda jest celowa i nie uprawnia organizatora do przetwarzania danych uczestników w innych celach. Oznacza to, że jeżeli organizator chciałby przeprowadzić konkurs podczas którego będzie fotografował uczestników w taki sposób, że zdjęcia będą umożliwiały identyfikację, powinien uzyskać odrębną zgodę na ich upublicznienie[13]. W takim wypadku wskazane jest, aby dodatkowa zgoda została dodana w karcie lub formularzu zgłoszeniowym.

Jeżeli konkurs jest skierowany do uczestników małoletnich, należy rozważyć możliwość samodzielnego zgłoszenia i wyrażenia zgody przez takiego uczestnika w kontekście przepisów RODO, podatkowych, a także Kodeksu cywilnego. Jeżeli nagroda jest niewielkiej wartości, a wygrana nie będzie rodzić dla zwycięzcy obowiązku podatkowego, dopuszczalne jest przyjmowanie zgłoszeń od uczestników, którzy ukończyli 13 rok życia, traktując udział w konkursie jako drobną sprawę życia

[12] *Ochrona danych osobowych w szkołach i placówkach oświatowych – poradnik*, https://uodo.gov.pl/pl/p/ochrona-danych-osobowych-w-szkolach-i-placowkach-oswiatowych-poradnik, s. 35, [dostęp 30.09.2019].

[13] W prawie autorskim przewidziano sytuacje, w których organizator może rozpowszechniać wizerunek uczestników bez ich zgody, porównaj z podrozdziałem: 9.4.

codziennego, zgodnie z przepisami Kodeksu cywilnego. W przeciwnym wypadku zalecane jest przyjęcie zasady, że zgodę na udział dziecka w konkursie wyraża jego opiekun ustawowy.

Organizator powinien wymagać od uczestników, na etapie przyjmowania zgłoszeń, jedynie minimalnego i niezbędnego zakresu danych (art. 5 RODO): jak imię, nazwisko, dane kontaktowe (telefon, adres e-mail), w przypadku kategorii wiekowych, wiek uczestnika (ale nie datę urodzenia). Jeżeli zamierza nagrody przekazywać drogą pocztową, to dane korespondencyjne powinien pozyskać jedynie od zwycięzców, po powiadomieniu o wygranej.

IV. Bezpieczeństwo przetwarzanych danych.

Obowiązkiem organizatora konkursu jest zapewnienie bezpieczeństwa gromadzonych i otrzymanych danych uczestników. Bezpieczeństwo należy zapewnić nie tylko poprzez środki techniczne, jak odpowiednie punkty przyjęć zgłoszeń, szafki zamykane na klucz służące do ich przechowywania, certyfikat SSL na stronie internetowej, ale także poprzez środki organizacyjne jak upoważnienie osób, które będą przyjmowały zgłoszenia do przetwarzania danych osobowych w tym celu oraz zobligowanie ich do zachowania poufności.

V. Udział innych podmiotów w przeprowadzanym konkursie.

Jeżeli konkurs będzie współorganizowany przez inny podmiot, niezbędne jest określenie obowiązków współadministratorów, w tym sposobu realizowania praw osób, których dane dotyczą przez każdego z nich. Co do zasady, niezbędne uzgodnienia pomiędzy współorganizatorami mogą być zawarte w regulaminie konkursu lub w umowie o współadministrowanie. Może też dochodzić do powierzenia czynności związanych z przeprowadzaniem konkursu innym podmiotom, np. szkołom, które zbiorą zgłoszenia. Do powierzenia dochodzi także przy konkursach wieloetapowych, gdzie zgłoszenia są przyjmowana na poziomie gminy, a najlepsze osoby z gminy, przechodzą do kolejnych etapów, powiatowego oraz wojewódzkiego. W takim wypadku biblioteka wojewódzka, jako organizator powierza przetwarzanie danych bibliotekom powiatowym oraz gminnym, które przeprowadzają poszczególne etapy konkursu.

Jeżeli zgłoszenia konkursowe są zbierane przez pracowników szkoły, która współpracuje z biblioteką, wskazane jest zawarcie umowy powierzenia danych osobowych na okoliczność stałej współpracy biblioteki ze szkołą. Umowa regulowałabym obowiązki szkoły, jako podmiotu przetwarzającego na okoliczność aktualnego, ale także przyszłych konkursów, jeżeli są realizowane na tych samych zasadach.

VI. Czas i sposób przechowywania danych.

Dane uczestników konkursu zawarte w karcie zgłoszeniowej organizator powinien przechowywać do zakończenia przewidzianego w regulaminie terminu na składanie reklamacji. Jeżeli zamierza w dalszym ciągu przetwarzać wizerunki tych uczestników to tak długo, jak będą te dane przetwarzane, jeżeli na karcie zgłoszeniowej jest zgoda na wykorzystanie wizerunku. Tutaj warto zwrócić uwagę, że w przypadku zgłoszeń elektronicznych, będzie to wymagało przechowywania informacji zapisanych w bazie danych.

Dane zwycięzców należy przechowywać przez okres wymagany przepisami podatkowymi (czyli co najmniej 5 lat kalendarzowych od następnego roku, po roku zakończenia konkursu).

Jeżeli praca konkursowa ma być wykorzystywana do promocji działalności biblioteki, np. poprzez jej wywieszenie, publikowanie na stronie internetowej lub zamieszczenie w wydawnictwie, należy przetwarzać dane tak długo, jak długo nie wygasną prawa autorskie do rozpowszechniania pracy lub praca nie będzie już wykorzystywana.

VII. Realizowanie obowiązków informacyjnych wobec uczestników i zwycięzców.

Podstawowym obowiązkiem biblioteki, jako organizatora konkursu jest przekazanie uczestnikom klauzuli informacyjnej. Zaleca się, aby pełna treść obowiązku informacyjnego z art. 13 ust. 1 i 2 RODO została zamieszczona w regulaminie konkursu, ponieważ uczestnik w każdej chwili ma dostęp do jego treści. Można treść klauzuli zamieścić także na karcie uczestnictwa, w całości lub najważniejsze informacje z odwołaniem do pełnej treści klauzuli w regulaminie.

9.3. Szczególne aspekty działalności biblioteki: Dyskusyjne Kluby Książki, Czytaki, zadania realizowane w ramach zewnętrznego dofinansowania.

Do zadań bibliotek, jako instytucji kultury, poza udostępnianiem materiałów bibliotecznych, należy także promocja czytelnictwa oraz edukacja. Często biblioteki realizują też działania mające na celu promocję gminy, wynikającą z przepisów o samorządzie gminnym. Wśród działań promocyjnych można wskazać w szczególności konkursy (omówione w podrozdziale 9.2), prowadzenie Dyskusyjnych Klubów Książki [DKK], wypożyczenie Czytaków, lekcje biblioteczne, spotkania autorskie. Większość działań promocyjnych wiąże się z koniecznością przetwarzania danych osobowych.

I. Dyskusyjne Kluby Książki.

DKK są formą promocji czytelnictwa, która została wymyślona i wypromowana przez Instytut Książki. Szczególną rolę w dziedzinie promocji czytelnictwa wśród Polaków, uzyskały w związku z dofinanoswaniem ich działalności przez Ministerstwo Kultury i Dziedzictwa Narodowego, w ramach „Programu dotacyjnego DKK". W Programie mogą brać udział biblioteki wojewódzkie, które z uzyskanych środków, wspierają działalność Klubów funkcjonujących przy bibliotekach.

Na wstępie należy zauważyć, że DKK nie jest częścią biblioteki. Jest to klub stworzony przez miłośników książek, w celu prowadzenia regularnych spotkań i dyskusji poświęconych książkom. Pierwsze DKK były inicjatywą prywatną i niezależną od bibliotek. DKK działające przy bibliotekach, w dalszym ciągu są odrębną jednostką, która jedynie działa przy bibliotece, korzystając z jej wsparcia i zasobów, pozostaje jednak zupełnie niezależna. Należy podkreślić, że działalność Klubów ma zupełnie prywatny charakter, nie podlega więc rygorom przepisów RODO, w szczególności nie mają statusu administratora danych i nie realizują obowiązków informacyjnych wobec członków.

W praktyce dyrektorzy bibliotek udzielają wsparcia DKK, aby skuteczniej upowszechniać czytelnictwo. Jednak każde wykorzystanie danych osobowych członków DKK, np. tworzenie list obecności, koordynowanie spotkań poprzez przekazywanie wiadomości e-mail, upublicznianie zdjęć ze spotkań; będzie podlegało wszystkim wymaganiom przepisów RODO, w szczególności konieczności spełnienia jednego z warunków legalizujących przetwarzanie z art. 6 ust. 1 RODO. Biorąc pod uwa-

gę status i sposób działania Klubów, należy uznać, że jedyną przesłanką legalizującą przetwarzanie danych osobowych ich członków będzie dobrowolna zgoda (art. 6 ust. 1 lit. a RODO). Jednocześnie należy podkreślić, że zgodnie z motywem 32 RODO, na tożsame cele przetwarzania wystarczy jedna zgoda i jest ona ważna aż do odwołania, czyli zgodę członka klubu wystarczy pozyskać tylko raz, jeżeli cel lub cele przetwarzania nie ulegną zmianie.

Programy dotacyjne wspierające DKK mają na celu finansowanie zakupu książek, spotkań z autorami, wydarzeń promujących czytanie, jak publiczne czytanie. Z ich realizacji beneficjenci środków przekazują do koorydnatora (Instytut Książki) sprawozdania statystyczne. Podkreślenia wymaga fakt, że samo rozliczenie pozyskanych środków, w tym przygotowanie sprawozdania, zgodnie z Regulaminem programu, nie wymaga udostępniania danych osobowych członków klubów w żadnej formie. Jednakże w wielu wypadkach pracownicy biblioteki wojewódzkiej zwracają się do bibliotek, przy których działają DKK z prośbą o przekazanie zdjęć ze spotkań. Takie zdjęcia mogą zostać udostępnione, jeżeli członkowie, których wizerunki zostały utrwalone, wyrazili na to zgodę lub na przekazanych zdjęciach nie ma wizerunku. Dalsze przekazanie zdjęć do Instytutu Książki także wymaga uprzedniej zgody członków Klubu. Poza pozyskaniem zgody, należy zrealizować obowiązek informacyjny z art. 13 ust. 1 i 2 RODO wobec członków Klubu.

Nie ma uzasadnienia dla udostępniania list uczestników spotkań lub danych członków klubu innym podmiotom, niż ten przy którym został utworzony DKK, w celu wykazania, że spotkanie faktycznie się odbyło. Nie byłoby to zgodne z zasadami przetwarzania danych osobowych z art. 5 RODO, tzn. adekwatności przetwarzania danych do celu. Ponieważ wszelkie sprawozdania mają charakter statystyczny, a zbieranie danych do celów dowodowych, gdy potrzebne są tylko dane statystyczne, miałoby nadmiarowy charakter.

W wielu przypadkach działalność DKK jest wspierania przez koordynatora, którego dane są publikowane na stronie biblioteki, przy której działa klub, w celu ułatwienia kontaktu. Takie działanie nie wymaga zgody pracownika, ponieważ mieści się w prawnie usprawiedliwionym interesie biblioteki (art. 6 ust. 1 lit. f RODO). Publikowanie wizerunku koordynatora, także utrwalonego podczas spotkań klubu, co do zasady wymaga pozyskania jego zgody, najlepiej w formie pisemnej[14].

II. „Czytaki" oraz inne materiały udostępniane osobom niepełnosprawnym.

Rozwój nowych technologii wpływa na sposób prowadzenia działalności przez biblioteki, które stają się coraz bardziej otwarte na książki elektroniczne i audio. Takie działania sprzyjają zmniejszaniu wykluczenia społecznego osób niepełnosprawnych, które nie mogą korzystać z tradycyjnych materiałów bibliotecznych. Czytelnik może wypożyczyć w bibliotece urządzenia służące do odczytu e-booków oraz różnego rodzaju audiobooków, a także materiały biblioteczne w formie cyfrowej. Jednym z takich urządzeń są „Czytaki" oraz książki mówione na te urządzenia, bezpłatnie udostępnianie przez Stowarzyszenie „Larix". Sposób korzytania z „Czytaków" istotnie różni się od innych repozytoriów dostępnych w bibliotece, ponieważ są to utwory, które zostały na podstawie przepisów art. 33[1] prawa autorskiego stworzone w formie cyfrowej, spejcalnie na użytek osób niepełnosprawnych. Powołanie się na ten przepis, oznacza konieczność wykazania przez organizację, która zwielokrotniła utwór, a także go udostępnia, że faktycznie jest to realizowane dla dobra osób niepełnosprawnych. Udostępnienie „Czytaków" bibliotece odbywa się na podstawie zawartego ze stowarzyszeniem porozumienia, w którym jako cel działania obu stron wskazano wspieranie osób niepełnosprawnych, a biblioteka jako beneficjent otrzymujący nagrania zobowiązuje się udostępniać je bezpłatnie tylko

[14] Porównaj podrozdział 9.4.

osobom niewidomym i słabowidzącym. Powyższe porozumienie nie daje uprawnienia do przetwarzania danych osobowych szczególnych kategorii, jakim jest stan zdrowia czytelnika.

W celu zrealizowania umownego zobowiązania, niezbędne jest spełnienie jednego z warunków legalności przetwarzania szczególnych kategorii danych, określonych w art. 9 ust. 2 RODO. Co do zasady, jedyną przesłanką legalizującą weryfikowanie, czy czytelnik chcący korzystać z „Czytaków" jest osobą niewidomą lub słabowidzącą, jest uzyskanie od niego pisemnej zgody na przetwarzanie informacji o jego stanie zdrowia. Potwierdzenie, że jest osobą niewidomą lub słabowidzącą czytelnik powinien złożyć w formie pisemnego oświadczenia, bez potrzeby okazywania zaświadczenia o niepełnosprawności. Warto także zwrócić uwagę na techniczny aspekt, utrudniający zadośćuczynienie obowiązkowi z art. 9 ust. 2 lit. a RODO. Jeżeli osoba niewidoma lub słabowidząca nie jest z opiekunem, który może pomóc jej złożyć stosowne oświadczenie, można podważyć jego autentyczność, stwierdzając, że nie wiedziała co podpisała. W bibliotece powinno się dołożyć należytej staranności, aby dać osobie, której dane dotyczą możliwość zapoznania się z treścią zgody, obowiązku informacyjnego, a także regulaminem korzystania z Czytaków. Powinny być one dostępne na przykład w języku Braille, nagrania głosowego, czy elektronicznie (z możliwością powiększenia czcionki, ale także odczytania tekstu). Wyrażenie zgody może wówczas nastąpić z wykorzystaniem podpisu elektronicznego, ePUAP, nagrania głosowego lub na karcie zgody napisanej w języku Braille.

Należy zwrócić uwagę, że karty czytelników korzystających z „Czytaków" powinny stanowić osobny podzbiór, do którego dostęp ma tylko bibliotekarz upoważniony do przetwarzania danych osobowych szczególnych kategorii w ramach czynności przetwarzania związanej z obsługą czytelników.

III. Zadania realizowane w ramach zewnętrznego dofinansowania.

Niektóre działania biblioteczne są realizowane w ramach zewnętrznego dofinansowania. Mogą to być programy ministerialne, np. „Kraszewski. Komputery dla bibliotek" lub „DKK"; środki przekazane przez fundacje i stowarzyszenia, np. realizowany w latach 2009-2019 Program Rozwoju Bibliotek; ale także środki z urzędu lub prywatnych sponsorów. Czasami skorzystanie ze środków finansowych jest obarczone podjęciem konkretnych działań związanych z przetwarzaniem danych osobowych, np. szkolenia lub konkursy. W ramach podpisywanego porozumienia, biblioteka jako beneficjent środków, jest zobligowana do przekazania materiałów potwierdzających ich właściwe wykorzystanie. Często za przekazaniem środków finansowych kryje się także cel promocyjny, gdzie sponsor wymaga, aby na stronach internetowych biblioteki zostały udostępnione zdjęcia ze zorganizowanych z wykorzystaniem uzyskanych środków wydarzeń, a także udostępnienia tych zdjęć do realizowania celu promocyjnego sponsora.

W każdym takim procesie, już na etapie negocjowania porozumienia, niezbędny jest udział inspektora ochrony danych. Powinien on ocenić ryzyka wiążące się ze spełnieniem wymagań wynikających z porozumienia, a także właściwie wymodelować przyszłe procesy przetwarzania, tak aby upublicznianie zdjęć zawierających zdjęcia uczestników lub przekazywanie list uczestników sponsorowi było możliwe. Obowiązkiem inspektora jest także analiza, czy zakres danych, których udostępnienia żąda sponsor, jest adekwatny do deklarowanego w porozumieniu celu przetwarzania danych. Jeżeli dane osobowe uczestników organizowanych przez bibliotekę wydarzeń mają być udostępniane zewnętrznym podmiotom, w prawnym interesie biblioteki, jako administratora jest pozyskanie zgody na przetwarzanie od uczestników lub ich opiekunów ustawowych (w przypadku małoletnich) w sposób umożliwiający wykazanie, że zgoda została wyrażona świadomie i dobrowolnie[15]. W takim przypadku zgoda musi obejmować także zgodę na dalsze udostępnienie danych, ze wskazaniem

[15] Nie dotyczy sytuacji, gdy przetwarzanie wizerunku opiera się na przesłankach legalności wskazanych w prawie autorskim, porównaj podrozdział 9.4.

podmiotu (odrębnego administratora), któremu dane zostaną udostępnione oraz znanych celów przetwarzania tych danych, np. Zamieszczenie w materiałach promocyjnych sponsora. To na bibliotece, jako pierwotnym administratorze ciąży obowiązek wykazania, że została uzyskana zgoda, także na żądanie sponsora, więc istotnym elementem jest także ustalenie, jak długo sponsor będzie przetwarzał (rozpowszechniał) udostępnione dane, ponieważ tak długo trzeba będzie przechowywać zgody uczestników wydarzenia. Należy pamiętać, że wykorzystanie wizerunku do celów promocyjnych co do zasady wiąże się z koniecznością zapłaty wynagrodzenia, dla osoby, której wizerunek utrwalono, więc zgoda powinna określać odpłatność lub nieodpłatność za upublicznienie wizerunku. Osoba, której dane dotyczą ma prawo w dowolnym momencie wycofać zgodę na przetwarzanie jej danych. W takim wypadku, należy niezwłocznie powiadomić wszystkich administratorów o żądaniu osoby, której dane dotyczą (art. 17 ust. 2 RODO).

9.4. Wykorzystanie wizerunków osób.

Wizerunek osoby (podobizna danej osoby utrwalona poprzez fotografię, rysunek czy obraz) stanowi jej dane osobowe. Zgodnie bowiem z art. 4 pkt 1 RODO dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

Wizerunek osoby należy zaliczyć do kategorii danych osobowych zwykłych. Stąd też przetwarzanie wizerunku osoby możliwe jest w przypadku istnienia podstawy prawnej – spełnienia jednej z przesłanek określonych w art. 6 ust. 1 RODO.

Należy zwrócić uwagę, że wizerunek osoby w postaci fotografii twarzy tej osoby może w pewnych sytuacjach być uznany za dane biometryczne (zgodnie z art. 4 pkt 14 RODO dane biometryczne oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne) jeśli przetwarzanie tego wizerunku odbywa się przy użyciu technik biometrycznych. W przypadku uznania wizerunku twarzy danej osoby za dane biometryczne przetwarzanie tego wizerunku możliwe jest w przypadku spełnienia jednej z przesłanek określonych w art. 9 ust. 2 RODO, stanowiących podstawę prawną przetwarzania szczególnych kategorii danych osobowych. Wykorzystywanie wizerunku osób, np. poprzez rozpowszechnianie tego wizerunku na tablicy ogłoszeń, w informatorze czy na stronie internetowej biblioteki stanowi przetwarzanie wizerunku osób. Stąd też przy wykorzystywaniu wizerunku osób znajdują zastosowanie przepisy RODO odnoszące się do przetwarzania danych osobowych.

Najczęstszą podstawą prawną przetwarzania wizerunku osoby może być zgoda udzielona przez tę osobę. Zgoda taka powinna spełniać warunki określone w art. 7 RODO. W szczególności ze zgody takiej powinno wynikać w jaki sposób wizerunek osoby będzie przetwarzany (wykorzystywany). Administrator powinien zawsze uzyskać zgodę na wykorzystanie wizerunku w przypadku jeśli fotografia, którą zamierza wykorzystać przedstawia jedną osobę, a zwłaszcza jeśli jest to fotografia portretowa (niezależnie do sytuacji w jakiej fotografia ta została wykonana). Dotyczy to także fotografii grupowych pozowanych, w szczególności gdy fotografie te opatrzone są opisem osób na nich się znajdujących. Przykładowo administrator powinien uzyskać zgodę osoby w przypadku jeśli zamierza wykorzystać jej wizerunek w postaci fotografii poprzez zamieszczenie tej fotografii w celach informacyjnych na swojej stronie internetowej czy profilu w serwisie społecznościowym. Zgody wymagać będzie także wykorzystanie w podobny sposób wizerunku osoby w postaci fotografii uczestnika szkolenia czy też konkursu organizowanego przez bibliotekę.

Wyjątki od zasady obowiązku uzyskania zgody na wykorzystanie wizerunku osoby przewidują przepisy ustawy o prawie autorskim. Zgodnie z art. 81 ust. 1 ustawy o prawie autorskim w braku wyraźnego zastrzeżenia zezwolenie (zgoda) nie jest wymagane, jeżeli osoba otrzymała umówioną zapłatę za pozowanie. Ponadto, zgodnie z art. 81 ust. 2 ustawy o prawie autorskim, zezwolenia nie wymaga rozpowszechnianie wizerunku:

a. osoby powszechnie znanej, jeżeli wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych,
b. osoby stanowiącej tylko szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza.

Z powyższego wynika, że administrator nie musi uzyskiwać zgody w przypadku wykorzystywania wizerunku osoby powszechnie znanej. Przy czym zasada ta nie dotyczy osób znanych w całej Polsce, czy nawet w mniejszym lub większym regionie kraju, wystarczy , aby dana osoba z racji pełnionych funkcji była znana osobom ze środowiska, w którym się obraca[16]. Stąd też nie wymaga zgody wykorzystanie przez bibliotekę wizerunku wójta, burmistrza, prezydenta, starosty, przewodniczącego rady, lokalnego działacza samorządowego czy społecznego.

Administrator nie musi uzyskiwać zgody w przypadku wykorzystywania wizerunku osób, które są uczestnikami wydarzeń publicznych (imprez publicznych, zgromadzeń), w szczególności organizowanych przez administratora), gdy stanowi on jedynie szczegół całości, tzn. służy zaprezentowaniu wydarzenia, a nie uczestników tego wydarzenia. Z kolei przesłanka krajobrazu oznacza, że rozpowszechnianie (wykorzystywanie) wizerunku nie wymaga zezwolenia, jeśli wizerunek osoby stanowi jedynie pewien element przedstawionej całości, tzn. w razie usunięcia wizerunku nie zmieniłby się przedmiot i charakter przedstawienia. Natomiast jeżeli elementem dominującym kadru jest wizerunek konkretnej osoby (fotograf skupia się na jednej osobie, eksponuje ją), rozpowszechnianie wymaga zgody osoby przedstawionej w kadrze[17]). Oznacza to, że w przypadku fotografii przedstawiających jedną osobę, nawet jeśli jest to fotografia wykonana w trakcie wydarzenia publicznego, w celu wykorzystania tej fotografii (wykorzystania wizerunku osoby) administrator musi uzyskać zgodę tej osoby. Podstawę prawną przetwarzania wizerunku osoby mogą stanowić także przepisy prawa. Przykładowo możliwość przetwarzania wizerunku pracownika przewidują przepisy Kodeksu pracy. Zgodnie z art. 22^1 § 4 Kodeksu pracy pracodawca żąda podania innych danych osobowych niż określone w art. 22^1§ 1 i 3 Kodeksu pracy (a więc także przykładowo fotografii przedstawiającej wizerunek pracownika), gdy jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Ponadto jak stanowi art. 22^{1b} § 2 Kodeksu pracy przetwarzanie danych biometrycznych pracownika (w tym wizerunku twarzy) jest dopuszczalne także wtedy, gdy podanie takich danych jest niezbędne ze względu na kontrolę dostępu do szczególnie ważnych informacji, których ujawnienie może narazić pracodawcę na szkodę, lub dostępu do pomieszczeń wymagających szczególnej ochrony. Powyższe przepisy Kodeksu pracy nie uprawniają jednak biblioteki do wykorzystania fotografii pracownika w celach informacyjnych: w identyfikatorach, wizytówkach czy na stronie internetowej biblioteki. Takie wykorzystanie wizerunku wymaga uzyskania uprzedniej zgody na przetwarzanie wizerunku pracownika.

Niezależnie od podstawy prawnej wykorzystania wizerunku osoby administrator musi spełnić w stosunku do osoby (osób), których wizerunek przetwarza obowiązek informacyjny, zgodnie z art. 13 RODO. Przykładowo może nastąpić to poprzez przekazanie pisemnej informacji (klauzuli informacyjnej) (należy w tym przypadku pamiętać o konieczności uzyskania pisemnego potwierdzenia przekazania takiej informacji najlepiej w postaci podpisu osoby, której informacja została przekazana, na wydruku klauzuli). W przypadku przetwarzania wizerunku na podstawie zgody spełnienie obo-

[16] Zobacz Wyrok Sądu Apelacyjnego w Krakowie z dnia 22 marca 2018 r., I ACa 1215/17, niepubl.
[17] Zobacz Wyrok Sądu Apelacyjnego w Warszawie z dnia 6 lutego 2018 r., V ACa 1040/17, niepubl.

wiązku informacyjnego powinno nastąpić w momencie uzyskania zgody, w przypadku przetwarzania wizerunku na podstawie przepisu prawa – w momencie uzyskania fotografii danej osoby.

9.5. Korzystanie z usług w chmurze.

Chmura obliczeniowa (również przetwarzanie w chmurze lub *cloud computing*) to model przetwarzania oparty na użytkowaniu usług dostarczonych przez usługodawcę (wewnętrzny dział lub zewnętrzna organizacja), bez konieczności zakupu licencji, instalowania i administrowania oprogramowaniem. Usługobiorca płaci jedynie za użytkowanie (dostęp do) określonej usługi. Termin powiązany jest z pojęciem wirtualizacji. Polega to na elektronicznym przetwarzaniu danych za pomocą usług dostępnych zdalnie przez sieć komputerową i/lub Internet.

Usługa chmury obliczeniowej jest wykorzystywana przez większość organizacji na świecie. Firmy, przedsiębiorstwa, urzędy i instytucje korzystają z niej na co dzień. Wysyłanie wiadomości e-mail, edytowanie dokumentów, oglądanie telewizji i słuchanie radia, słuchanie muzyki, oglądanie filmów, granie czy przechowywanie danych, jest dzisiaj w większości oparte o usługi chmurowe. Inne zastosowania chmury obliczeniowej to także tworzenie nowych aplikacji i usług, wykonywanie i odzyskiwanie kopii zapasowych danych, analizowanie danych, przesyłanie strumieniowe audio i wideo. Coraz częściej używa się chmury obliczeniowej nawet nie zdając sobie z tego sprawy, ponieważ umożliwia szybką i wydajną pracę. Koszty tej usługi są mniejsze niż tradycyjne rozwiązanie, wymagające zakupu sprzętu komputerowego/serwerów wraz z oprogramowaniem, budowa i modernizacja własnej sieci informatycznej, a także zaangażowanie zasobów ludzkich i finansowych. Niskie koszty przy bardzo dużej wydajności składają się na popularność tego rozwiązania. Chmury obliczeniowe bardzo ułatwiły codzienne życie i odmieniły cyfrowy świat.

I. Zasada działania chmury obliczeniowej.

Usługa chmurowa polega na przeniesieniu ciężaru świadczenia usług informatycznych (danych, oprogramowania lub mocy obliczeniowej) na serwer i umożliwienie stałego dostępu do niego. Wystarczy zalogować się z jakiegokolwiek urządzenia z dostępem do Internetu, by zacząć korzystać z usług w chmurze. Chmura obliczeniowa jest nieograniczonym zasobem informatycznym. Najprościej mówiąc, chmura obliczeniowa to dostarczanie usług obliczeniowych, w tym serwerów, powierzchni dyskowych, procesorów, pamięci, baz danych i ich analizy oraz oprogramowania za pośrednictwem Internetu.

Chmury dzielimy na trzy rodzaje:

a. publiczne, będące zewnętrznym, ogólnie dostępnym dostawcą, są własnością firm zewnętrznych i są dostępne dla każdego, kto chce z nich korzystać,
b. prywatne tworzone w obrębie własnej sieci komputerowej organizacji i tylko w niej udostępniane,
c. hybrydowe będące połączeniem chmury prywatnej i publicznej. Część aplikacji i infrastruktury pracuje w chmurze prywatnej, a część w przestrzeni publicznej.

II. Modele chmur obliczeniowych.

Zasadniczo możemy podzielić rodzaje usług chmury obliczeniowej według zasady jej działania. Obecnie wyróżnia się następujące modele:

a. Kolokacja, która polega na wynajęciu pomieszczenia serwerowni z dostępem do energii, klimatyzacji i Internetu. Pozostałe składniki są po stronie usługobiorcy.
b. Serwery (IaaS) czyli „infrastruktura jako usługa"– usługobiorca odpowiada za oprogramowanie, a dostawca zapewnia sprzęt.
c. Platforma (PaaS) czyli „platforma jako usługa"– podobnie jak serwery, jednak tu usługodawca dostarcza także środowisko programistyczne.
d. Oprogramowanie (SaaS) czyli „oprogramowanie jako usługa"– w tym przypadku korzysta się z gotowego produktu, a dostawca zajmuje się wszystkim: sprzętem, systemem, środowiskiem programistycznym i aplikacjami.
e. Komunikacja (CaaS) czyli „komunikacja jako usługa" tu usługodawca zapewnia platformę pod telekomunikacyjne środowisko pracy.
f. Platforma integracyjna (IpaaS) czyli „platforma integracyjna jako usługa" tu zapewnia się platformę do integracji pomiędzy różnymi usługami w chmurze.

III. Wady i zalety usług chmurowych.

Jedną z największych zalet chmury obliczeniowej jest mobilność, czyli ułatwiona dostępność do zasobów z dowolnego miejsca na świecie z różnych urządzeń (PC, laptop, tablet, smartfon) z dostępem do Internetu. Poprawia to komunikację w firmie oraz współpracę poza nią. Daje także swobodę dzielenia się danymi. Przetwarzanie danych w chmurze to także optymalizacja kosztów, poprzez zmniejszenie potrzeby utrzymywania danych na własnym sprzęcie oraz odciążeniu firmowych serwerów. Zmniejszenie także wydatków na utrzymanie sprzętu, wykupienie aktualizacji oprogramowania oraz licencji na systemy i aplikacje. Przeniesienie usługi do chmury zapewnia także niezawodność i niezależność od awarii sprzętu. Przechowywanie danych w chmurze pozwala zachować ciągłość działania. Stanowi dodatkowe zabezpieczenie, które chroni przed nieodwracalnymi skutkami awarii. Chmura obliczeniowa pozwalana na tworzenie kopii zapasowych, odzyskiwanie danych po awarii, dzięki możliwości dublowania danych u usługodawcy. Odpowiednio dobrana usługa daje wysokie gwarancje bezpieczeństwa. Standardem jest szyfrowanie wszelkiego transferu danych do i z chmury, a także szyfrowanie danych przechowywanych w chmurze przez usługodawcę. Profesjonalne firmy oferujące usługi chmurowe, zatrudniają specjalistów czuwających nad bezpieczeństwem powierzonych danych. Dodatkowo dostawcy oferują technologie i środki zwiększające poziom bezpieczeństwa i chroniące przed zagrożeniami. Skalowalność chmury obliczeniowej pozwala dobrać odpowiednią ilość zasobów. Usługi świadczone w chmurze są dostępne non stop, z każdego urządzenia. Warto także zwrócić uwagę na kwestię ochrony środowiska. Centra danych potrzebują dużo sprzętu i zużywają ogromne ilości prądu. Jednak jest to mniej niż w przypadku wielu komputerów biurowych. Dostawcy usług chmurowych, potrafią zoptymalizować centra pod kątem wykorzystania energii. Jest to rozwiązanie, ograniczające emisję dwutlenku węgla oraz zasobów prądu czy paliwa, czyli jest znacznie bardziej przyjazne środowisku niż standardowe rozwiązania.

Pomimo wielu niezaprzeczalnych zalet, chmura obliczeniowa ma także kilka wad, wśród których należy wskazać zagrożenia dla bezpieczeństwa danych. Korzystanie z usług chmurowych wiąże się z potencjalnym ryzykiem, że do danych może mieć dostęp osoba niepowołana. Administrator może nie mieć pełnej wiedzy w zakresie miejsc przechowywania danych i tego, kto po stronie usługodawcy uzyskuje do nich wgląd. Warto także zwrócić uwagę na aspekt ograniczonej kontroli nad danymi w wypadku awarii u usługodawcy. Awaria może oznaczać utratę dostępu do danych. Zarówno w przypadku oprogramowania w chmurze, jak i własnego, większość przypadków złamania zabezpieczeń to wina błędów ludzkich. Jednak u dostawcy usług chmurowych zabezpieczenia są w rękach

specjalistów. Natomiast zróżnicowany poziom dostępności usług to drugi, obok bezpieczeństwa, najważniejszy problem dotyczący usług chmurowych. Jakość usług zazwyczaj jest ściśle powiązana z ceną, a ceny usług chmurowych sukcesywnie rosną. Zagrożeniem może być także wycofanie się z rynku dostawcy usług w chmurze lub zmiany oferowanych usług przez usługodawcę. To naturalne zjawisko na rynku, jednak może wiązać się z utratą rozliczalności danych. Samo korzystanie z rozwiązania chmurowego jest uzależnione od stabilności połączenia z Internetem. Wiele usług daje możliwość pracy także offline, jednakże prawdziwą wydajność i skuteczność gwarantuje jedynie stały i szybki dostęp do Internetu przez usługobiorcę.

IV. Korzystanie z usług chmurowych a przepisy RODO.

Jeżeli w bibliotece są wykorzystywane zewnętrzne usługi chmurowe, które wiążą się z przetwarzaniem danych, niezbędne jest upewnienie się, że korzystanie z tej usługi jest zgodne z wymaganiami przepisów o ochronie danych osobowych. W wyborze dostawcy należy kierować się nie tylko ceną usługi, ale także gwarancjami bezpieczeństwa i zgodności z przepisami, które usługodawca jest w stanie zapewnić. Analizę postanowień umownych oraz regulaminu powinien przeprowadzić nie tylko informatyk, ale także inspektor ochrony danych zatrudniony w bibliotece. Należy zwrócić uwagę, że korzystanie z usługi chmurowej wymaga zawarcia powierzenia danych osobowych, zgodnie z wymaganiami art. 28 RODO. Jeżeli dostawca odmawia zawarcia umowy powierzenia, nie powinno korzystać się z jego usług. Umowa może zostać zawarta na piśmie lub elektronicznie. Podmiot dostarczający usługę powinien zapewnić zgodność przetwarzania danych z przepisami RODO. Wskazane jest także dokonywanie wyboru dostawców, którzy gwarantują, że przetwarzanie danych odbywa się w krajach EOG lub spoza EOG, które zostały uznane przez Komisję Europejską za dające wystarczające gwarancje bezpieczeństwa. W przypadku amerykańskich usługodawców niezbędne jest posiadanie certyfikatu, gwarantującego przetwarzanie danych zgodnie z postanowieniami Tarczy prywatności UE-USA[18]. Warto zwrócić uwagę, że certyfikaty są przyznawane czasowo. Wybór dostawcy usługi chmurowej powinien być także oparty na stopniu bezpieczeństwa, jaki dostawca jest w stanie zapewnić. Odpowiednie gwarancje powinny być częścią umowy z usługodawcą, które są wyrażone w formie oświadczenia, o ile to możliwe popartego dowodami, np. uzyskanymi certyfikatami.

9.6. Wykorzystanie biometrii do kontroli dostępu.

I. Czym jest biometria.

Biometria to nauka zajmująca się badaniem zmienności populacji organizmów. To również technika dokonywania pomiarów istot żywych. W najnowszych zastosowaniach ukierunkowana jest na metody automatycznego rozpoznawania ludzi na podstawie ich cech fizycznych.

Biometryczne metody badają cechy fizyczne, np. tęczówka oka, siatkówka (dno oka), charakterystykę linii papilarnych, układ naczyń krwionośnych na dłoni lub przegubie ręki, palcu czy nadgarstku, kształt dłoni, kształt linii zgięcia wnętrza dłoni, kształt ucha, kształt twarzy, rozkład temperatur na twarzy, kształt i rozmieszczenie zębów, zapach, DNA. Biometria bada również cechy behawioralne, tzn. związane z zachowaniem, np. sposób chodzenia, podpis odręczny, pismo ręczne, sposób pisa-

[18] Lista podmiotów jest udostępniona publicznie pod adresem: https://www.privacyshield.gov/list

nia na klawiaturze komputera, sposobu uderzania w klawisze, głos, a nawet sposób reakcji mózgu, na pewne znane informacje-bodźce. Biometryczne techniki w praktycznych zastosowaniach zajmują się przede wszystkim weryfikacją osób. Czyli jest to technika identyfikacji organizmów żywych, która opiera się na mierzalnych cechach fizycznych i behawioralnych. Technologia biometryczna umożliwia identyfikowanie osoby po analizie indywidualnych cech fizycznych, które są dla każdego z nas unikalne.

Najstarsze dowody na zastosowanie biometrii pochodzą z prehistorii, gdzie za pomocą odcisku dłoni artyści podpisywali swoje dzieła na ścianach jaskiń. Późniejsze dowody pochodzą ze starożytnej Babilonii, gdzie odciskami palców w glinianych tabliczkach potwierdzano transakcje handlowe. Z kolei jako metoda weryfikacji tożsamości została pierwszy raz użyta w XIX w., kiedy to Imperium Brytyjskie znalazło sposób na demaskowanie oszustów poprzez identyfikację na podstawie porównania linii papilarnych. Technologia biometryczna we współczesnym rozumieniu pojęcia została zastosowana w Japonii i Kolumbii dopiero w 2004 r.

Obecnie stosowane klasyczne metody kontroli dostępu identyfikują kartę, numer czy hasło. Uwierzytelnianie związane jest z urządzeniem, a nie człowiekiem. Jednakże biometria znajduje coraz częstsze zastosowanie w nowoczesnych technologiach. Wykorzystywana jest jako sposób kontroli dostępu do pomieszczeń i obiektów, do autoryzacji osób korzystających z urządzeń, programów, zasobów takich jak informacje czy dane. Podstawową jej funkcją jest więc uniemożliwianie realizacji nieautoryzowanego dostępu do chronionych zasobów. Wspomaga wyszukiwanie miejsca pobytu osób, czy rejestrację czasu pracy. Usprawnia obsługę w instytucjach, zmniejszając liczbę papierowej dokumentacji oraz przyspieszając obieg dokumentów. Techniki biometryczne nadają się do zabezpieczania obiektów, pojedynczych urządzeń i zasobów. Biometrię twarzy, czy zgodność odcisku palca wykorzystują coraz częściej komputery i smartfony, do autoryzacji użytkownika. Dzięki połączeniu biometrii z podpisem elektronicznym możliwe jest sygnowanie w bezpieczny sposób dokumentów na linii klient-bank czy klient-urząd, gdzie zabezpieczenie ma na celu eliminację fałszerstw.

II. Techniki biometryczne.

Najpopularniejsze techniki biometryczne, ze względu na zastosowaną technikę weryfikacji tożsamości można podzielić następująco:

a. systemy rozpoznające na podstawie układu linii papilarnych – system sprawdza układ punktów charakterystycznych dla linii papilarnych oraz innych cech identyfikujących palec,
b. systemy rozpoznające na podstawie geometrii dłoni – wykonywanych jest ponad 90 pomiarów różnych cech charakterystycznych dłoni. Wynik jest przechowywany w formie wzorca unikalnego dla każdego człowieka,
c. systemy rozpoznające na podstawie brzmienia głosu – cechy fizyczne jak np. długość kanału głosowego, budowa i wielkość płuc, budowa tchawicy, kształt więzadeł głosowych, budowa krtani, ułożenie języka, budowa klatki piersiowej oraz sposób wypowiadania się, który jest charakterystyczny dla danej osoby (barwa, natężenie, głębia, wysokość głosu, głośność, tempo, artykulacja, wymowa, pauzy, rytmiczność) – tworzą niepowtarzalny wzorzec głosu każdego człowieka, dzięki biometrii głosowej czas weryfikacji tożsamości może być krótszy o 40%,
d. systemy rozpoznające na podstawie obrazu tęczówki oka – specjalna kamera wykonuje zdjęcie tęczówki o bardzo wysokiej rozdzielczości, następnie powstaje kod zawierający skrócony opis punktów charakterystycznych tęczówki, a w dalszej kolejności kod jest szyfrowany i porównywany z zaszyfrowanym kodem oryginału tęczówki zapisanym w bazie systemu,
e. systemy rozpoznające na podstawie unikalnego układu naczyń krwionośnych dłoni – wzorzec

zapisuje się w centralnej bazie danych lub w urządzeniu weryfikującym. Skanowanie naczyń krwionośnych odbywa się tzw. bliską podczerwienią. System porównuje zapisany wzorzec układu naczyń krwionośnych dłoni do wzoru naczyń krwionośnych dłoni zbliżonej do czytnika. Wzorzec ten jest unikalny dla każdego człowieka.

Zalety technologii biometrycznych to przede wszystkim bardzo wysoki poziom bezpieczeństwa ze względu na odporność na fałszerstwa, błyskawiczne potwierdzenie tożsamości, dające pewność, że autoryzacji dokonuje osoba uprawniona, nie tylko posiadająca identyfikator czy hasło. Zaletami są też brak potrzeby pamiętania haseł i ich zmieniania, a także noszenia kart identyfikacyjnych czy kluczy. Wśród innych zalet należy wskazać brak możliwości dzielenia się danymi biometrycznymi z inną osobą. Sama niezmienność danych biometrycznych, która jest też negatywną cechą (np. w przypadku ich kradzieży), jest co do zasady zaletą, w rozumieniu odporności metod biometrycznych, gdyż źródła pozyskania danych nie można usunąć. Dane biometryczne, nigdy się nie zmienią, np. nie można wymienić układu żył.

Biometria wydaje się być nieuniknionym trendem, a rozwiązania biometryczne konsekwentnie zastępują tradycyjne. Biometria w sposób prawie niezauważalny staje się jedną z głównych metod weryfikacji tożsamości. Powszechne stosowanie metod biometrycznych wiąże się z zabezpieczeniem osób i ich tożsamości w społeczeństwie informacyjnym, a metody te są jednymi z najbezpieczniejszych. Dzięki temu znajdują zastosowanie w różnych dziedzinach życia społecznego.

III. Legalność wykorzystywania danych biometrycznych a RODO.

W ustawie ODO nie odniesiono się do danych biometrycznych, jako danych wrażliwych, choć obejmują one informacje o cechach fizycznych, fizjologicznych oraz behawioralnych osoby, wobec czego powinny być lepiej chronione, niż zwykłe dane osobowe. Obecnie dane biometryczne są danymi szczególnej kategorii w rozumieniu art. 9 ust. 1 RODO. Zgodnie z art. 4 pkt 14 RODO dane biometryczne „oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne". Dane biometryczne w rozumieniu tego przepisu to dane, które spełniają jednocześnie trzy warunki: wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych oraz umożliwiają jednoznaczną identyfikację osoby. Zatem w rozumieniu przepisów RODO, danymi biometrycznymi są tylko te dane, które spełniają wszystkie trzy warunki łącznie.

Zgodnie z art. 9 ust. 1 RODO przetwarzanie danych szczególnych kategorii, w tym danych biometrycznych, jest zakazane. Jednakże zakaz przetwarzania tych danych nie jest bezwzględny. Przesłanki dopuszczalności przetwarzania szczególnych kategorii danych osobowych zostały wskazane w art. 9 ust. 2 RODO. Dodatkowo przepisy art. 9 ust. 4 RODO przyznają państwom członkowskim prawo wprowadzenia w prawie krajowym dodatkowych przesłanek od zakazu przetwarzania danych biometrycznych. Co do zasady w bibliotece biometria może być wykorzystywana do zabezpieczenia urządzeń należących do infrastruktury teleinformatycznej oraz dostępu do pomieszczeń, jeżeli jest to niezbędne ze względu na kontrolę dostępu do szczególnie ważnych informacji, których ujawnienie może narazić pracodawcę na szkodę, lub dostępu do pomieszczeń wymagających szczególnej ochrony (art. 221b § 2. Kodeksu pracy). Ze względu na charakter danych biometrycznych, wprowadzenie takiej metody kontroli dostępu musi zostać poprzedzone oceną skutków dla ochrony danych (art. 35 RODO). Stosowanie biometrii do kontroli czasu pracy wydaje się nieuzasadnione, ze względu na szczególny charakter przetwarzanych do tego celu danych (tzn. nieadekwatność danych do celu

przetwarzania według art. 5 RODO). W zasadzie jedyną przesłanką legalizującą wprowadzenie technologii biometrycznej do biblioteki, jest uzyskanie dobrowolnych i świadomych zgód na przetwarzanie danych osobowych, zgodnie z art. 9 ust. 2 pkt a RODO. Jednocześnie należy zaznaczyć, że pracodawca wychodzi z pozycji siły, więc może budzić wątpliwości, czy zgody pracowników faktycznie były dobrowolne. Przez dobrowolność należy także rozumieć to, że osoba, której dane będą przetwarzane, może nie wyrazić zgody na przetwarzanie jej danych biometrycznych, a także wycofać zgodę w dowolnym momencie. Oznacza to, że oparcie systemu zabezpieczeń (dostęp do sprzętu, dostęp do pomieszczeń) na biometrii będzie wymagało zastosowania alternatywnego rozwiązania, umożliwiającego wykonanie tych samych czynności bez zastosowania biometrii. Dla przykładu, większość urządzeń mobilnych oraz przenośnych, jak smartfony i laptopy umożliwia odblokowanie urządzenia z wykorzystaniem odcisku linii papilarnych lub zdjęcia twarzy. Takie rozwiązanie można zapewnić użytkownikom, jednak w bibliotece nie można zmusić ich do korzystania z niego. Biometria w świetle aktualnie obowiązujących przepisów może być narzędziem wspierającym system ochrony danych w bibliotece, jednak nie może zastąpić innych, tradycyjnych rozwiązań, które nie wymagają pozyskania zgody od osoby, której dane dotyczą.

Przetwarzając dane biometryczne należy pamiętać o podstawowych zasadach przetwarzania danych, jak adekwatność, proporcjonalność czy rozliczalność (art. 5 RODO). Odnosi się do tego również motyw 39 RODO wskazując, że „dane osobowe powinny być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są przetwarzane". Znaczy to, że wolno je przetwarzać tylko w wtedy, gdy celu przetwarzania nie można osiągnąć innymi sposobami.

Danych szczególnych dotyczy również motyw 51 RODO. Odnosi się on m.in. do przetwarzania fotografii. „Przetwarzanie fotografii nie powinno zawsze stanowić przetwarzania szczególnych kategorii danych osobowych, gdyż fotografie są objęte definicją danych biometrycznych tylko w przypadkach, gdy są przetwarzane specjalnymi metodami technicznymi, umożliwiającymi jednoznaczną identyfikację osoby fizycznej lub potwierdzenie jej tożsamości". Czyli nie każde użycie fotografii zawierającej wizerunki lub inne cechy szczególne osób sfotografowanych, to przetwarzanie danych szczególnych. Przetwarzanie fotografii będzie przetwarzaniem danych biometrycznych, jeżeli jest dokonywane specjalnymi, zautomatyzowanymi, metodami technicznymi umożliwiającymi identyfikację lub potwierdzenie tożsamości osoby. Jeżeli urządzenia techniczne stosowane do monitoringu w bibliotece będą w stanie na podstawie nagrań identyfikować lub potwierdzać tożsamość osoby przebywającej na terenie biblioteki, to takie zautomatyzowane przetwarzanie będzie przetwarzaniem danych biometrycznych i może odbywać się wyłącznie po spełnieniu warunków dopuszczalności określonych w art. 9 RODO.

Powszechne stosowania metod biometrycznych stwarza problem naruszania prywatności. W sytuacji stosowania ich bez odpowiednich zabezpieczeń i przesłanek legalizujących działanie, prawo do ochrony danych osoby jest zagrożone. W związku z tym technologie biometryczne stanowią szczególe zagrożenie dla ochrony danych i prywatności osoby. Biorąc to pod uwagę zdefiniowano je osobno od innych danych (art. 4 pkt 14 RODO) oraz zakwalifikowano do szczególnych kategorii danych osobowych (art. 9 RODO). Osobno został zdefiniowany cel i zakres ich przetwarzania oraz wynikające z tego zagrożenia. Wobec powyższego każdy przypadek przetwarzania danych biometrycznych należy traktować indywidualnie i poprzedzić odpowiednią oceną skutków dla ochrony danych (art. 35 RODO).

IV. Wady korzystania z biometrii.

Biometria to nie tylko innowacyjność, to także wygoda. Jednym z celów wprowadzania systemów biometrycznych jest uproszczenie, czy ułatwienie pracy. Wykorzystanie biometrii do logowania lub

kontroli dostępu przyśpiesza te procesy, zmniejsza też ryzyko pomyłki lub nieuprawnionego uwierzytelnienia. Dotychczasowe systemy zabezpieczeń i narzędzia autoryzacji cechują liczne wady, jak podatność na phishing, kradzież lub złamanie hasła. Dane biometryczne podwyższają poziom bezpieczeństwa oraz upraszczają identyfikację. Uwierzytelnianie jest łatwiejsze, szybsze i wygodniejsze. Są to też rozwiązania coraz bardziej przystępne cenowo. Można zatem oczekiwać, że zabezpieczenia biometryczne będą dominować w przyszłości.

Jednak powszechne stosowane techniki biometryczne niesie nowe, nieznane zagrożenia. Tak jak dotychczasowe zabezpieczenia mają wady, tak zabezpieczenia biometryczne nie są ich pozbawione. Przede wszystkim różne metody, dają różny poziom zabezpieczenia. Użyteczność, społeczna akceptowalność, odporność na oszustwa, koszty czy bezpieczeństwo to cechy, od których zależy wybór danej metody. Wśród wad biometrii można wskazać brak przejrzystości (algorytmy i ocena zewnętrzna), możliwość błędnej identyfikacji, weryfikacji, klasyfikacji (różnica wzorca i próbki), podatność na łączenie danych (użycie takiego samego rodzaju danych biometrycznych może prowadzić do skojarzenia danych dotyczących tej samej osoby pochodzących z różnych systemów). Negatywną cechą jest też niezmienność wzorca, czyli gdy raz zostanie on wykradziony lub upubliczniony, to jego wykorzystanie do zabezpieczenia danych poprzez metodę biometryczną jest bezskuteczne. Wzorzec można także usunąć lub zmienić.

Warto także zwrócić uwagę na to, że urządzenie nie jest w stanie rozpoznać, czy ma do czynienia z prawdziwym człowiekiem, czy na przykład z bardzo dobrym odwzorowaniem. Gdyby system sprawdzał stuprocentową dokładność odczytywanych danych ze wzorcem, nigdy nie dokonałby autoryzacji. Przykładem jest czytnik linii papilarnych, gdyż praktycznie nigdy nie uda się w identyczny sposób przyłożyć palca do czytnika. Do opisu danej cechy biometrycznej używa się zwykle pewnej liczby cech. Różne sensory mają swoje wady i zalety, np. dla sensorów optycznych mogą to być zanieczyszczenie senosoru, łatwość oszukania, mała odporność mechaniczna, duża powierzchnia czytnika.

Biometria głosowa zależy od nastroju czy czynników zewnętrznych, jak choćby stan zdrowia. Niektóre cechy fizyczne czy behawioralne zależne są od samopoczucia osoby, np. głos, źrenica czy mimika twarzy. Należy także pamiętać, że stosowanie biometrii oznacza konieczność wprowadzenia wysokiej klasy zabezpieczeń wzorca. Ujawnienie danych biometrycznych może mieć bardzo negatywne skutki, dla osoby, której dane dotyczą. Dane genetyczne mogą ujawnić informacje (częściowe) o bliskich osoby, której dane dotyczą. Zagrożenia metod i systemów biometrycznych są zależne od zastosowanych środków i procedur bezpieczeństwa.

Biometria to krok w przyszłość w dziedzinie bezpieczeństwa. Z drugiej jednak strony istnieje ryzyko wykradnięcia bardzo prywatnych danych. Zabezpieczenia z dnia na dzień ewoluują. Poprzeczka dotycząca wymagań zabezpieczeń biometrycznych jest ustawiana coraz wyżej. Uwierzytelnianie użytkowników jest bezwartościowe, jeżeli ochrona jest słaba. Dlatego też ochrona jest zadaniem podstawowym. Projektowanie i zarządzanie systemem działającym w oparciu o metody biometryczne musi być integralną częścią ogólnego planu ochrony i planu ochrony sieci. Zabezpieczenia biometryczne zwiększają bezpieczeństwo, ale żadne z rozwiązań biometrycznych nie zapewni pełnego bezpieczeństwa.

9.7. Monitoring wizyjny.

Dyrektor biblioteki ma możliwość wprowadzenia szczególnego środka nadzoru, jakim jest monitoring wizyjny na podstawie przepisów art. 222 Kodeksu pracy, jeżeli jest to niezbędne do zapewnienia bezpieczeństwa pracowników, ochrony mienia, kontroli produkcji lub zachowania w tajem-

nicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę. Podstawą legalizującą przetwarzanie danych gromadzonych w ramach wideonadzoru jest art. 6 ust. lit. c RODO, ponieważ możliwość jego wprowadzenia wynika bezpośrednio z ustawy Kodeks pracy.

I. Uzasadnienie wyboru.

Dyrektor biblioteki musi być w stanie wykazać, że wprowadzenie monitoringu jest niezbędne, biorąc pod uwagę to, że jest to najlepszy dostępny środek techniczny zapewniający bezpieczeństwo. Ze względu na fakt, że biblioteki są miejscem publicznym, ogólnodostępnym, a także ograniczonymi możliwościami budżetowymi monitoring jest chętnie wybieranym przez nie środkiem nadzoru. Ze względu na fakt, że w ustawie Kodeks pracy wskazano, iż wprowadzenie monitoringu jest dozwolone jedynie wtedy, gdy jest niezbędne do realizacji wskazanych celów, biblioteka powinna udokumentować zasadność jego wprowadzenia. Dobrą praktyką jest przeprowadzenie konsultacji z pracownikami, w tym radą pracowniczą i związkami zawodowymi, jeżeli funkcjonują w bibliotece, a także przeprowadzenie konsultacji z użytkownikami. Warto napisać sprawozdanie z tych spotkań, szczególnie gdy pytani potwierdzają, że ich zdaniem funkcjonowanie monitoringu wpływa na poprawę ich poczucia bezpieczeństwa, a także zapewnienia nadzoru nad księgozbiorem oraz przetwarzanymi w bibliotece danymi. W uzasadnieniu wykorzystywania monitoringu w bibliotece dyrektor powinien także zawrzeć własne argumenty dotyczące zasadności stosowania wideonadzoru. W dużym zakładzie pracy bezpieczeństwo przeciwpożarowe także jest argumentem za wprowadzeniem monitoringu – w sytuacjach awaryjnych pozwala szybko sprawdzić, czy w miejscach zagrożenia nikt nie pozostał. Zalecane jest dokumentowanie zasadności wprowadzenia monitoringu także na wypadek kontroli ze strony organu nadzoru, który dokonuje oceny zgodności zastosowanych środków bezpieczeństwa z przepisami o ochronie danych osobowych. Jedną z form dokumentacji może być przeprowadzona na zasadach określonych w art. 35 RODO ocena skutków.

II. Umiejscowienie kamer.

W ustawie Kodeks pracy zostały określone strefy, w których wprowadzenie wideonadzoru jest niedozwolone w toaletach, pokojach socjalnych, stołówkach, palarniach, szatniach, a także pomieszczaniach, z których korzystają związki zawodowe. Jednakże możliwe jest odstępstwo od tej reguły, jeżeli istnieje wyższy interes pracodawcy, wymagający zapewnienia nadzoru w tych miejscach. W praktyce może to oznaczać, że ze względu na częste kradzieże mienia pracowników, zostanie zainstalowana kamera w szatni. Jednakże ze względu na ryzyko naruszenia prywatności pracowników, przed wprowadzeniem monitoringu kierownictwo biblioteki powinno przeprowadzić referendum wśród pracowników, którzy podejmą świadomą decyzję w tym zakresie. Spisanie wyników rozmów z pracownikami, będzie stanowiło dowód dla dyrektora biblioteki w zakresie zasadności podjętej przez niego decyzji o wprowadzeniu widonadzoru w jednym ze szczególnych miejsc. Należy także zwrócić szczególną uwagę na zasięg kamer, aby pomimo umieszczenia ich, np. w przejściach i korytarzach, nie obejmowały swym zasięgiem pomieszczeń określonych, jako niedozwolone.

III. Wykorzystanie nagrań.

Zabronione jest wykorzystywanie nagrań do innych celów, niż te wskazane w kodeksie pracy. W szczególności kamery nie mogą służyć do kontroli czasu pracy lub oceny jakości pracy pracowni-

ków. Nie może to być narzędzie nadzoru nad sposobem realizacji obowiązków przez pracowników. Takie wykorzystanie nagrań byłoby nie tylko naruszeniem przepisów ustawy Kodeks pracy, ale także zasady celowości przetwarzania danych osobowych, o której mowa w art. 5 RODO. Prawo do prywatności pracownika musi być bezwzględnie poszanowane przez pracodawcę.

IV. Obowiązek poinformowania pracowników o monitoringu.

Dyrektor biblioteki informuje pracowników o wprowadzeniu monitoringu nie później niż 2 tygodnie przed jego uruchomieniem, a jeżeli monitoring już funkcjonuje w bibliotece, powinien dopełnić tego obowiązku niezwłocznie. Informacja powinna być przekazana każdemu pracownikowi na piśmie, najlepiej z oświadczeniem o zapoznaniu się, aby kopię informacji można było dołączyć w celach dowodowych do akt pracownika. W związku z wprowadzeniem monitoringu należy także przekazać informacje o celu, zakresie oraz sposobie zastosowania monitoringu w układzie zbiorowym pracy lub w regulaminie pracy albo w obwieszczeniu, jeżeli pracodawca nie jest objęty układem zbiorowym pracy lub nie jest obowiązany do ustalenia regulaminu pracy (art. 22^2 § 6-7 ustawy Kodeks pracy).

V. Okres przechowywania nagrań.

Nagrania mogą być przechowywane maksymalnie przez 3 miesiące, jednakże w wielu współczesnych systemach nagrania są przechowywane o wiele krócej, ze względu na ogromne koszty z tym związane. Często są także stosowane systemy ciągłego nagrywania, w których nadpisywane są już zarejestrowane nagrania. W takim wypadku należy określić bardziej precyzyjnie czas przechowywania nagrań, np. nie krócej niż 3 dni nie dłużej niż 14 dni. Uzyskanie precyzyjnej informacji o okresie przechowywania danych jest istotne przy tworzeniu klauzuli informacyjnej.

VI. Nagrywanie dźwięku oraz cech szczególnych.

Niedozwolone jest stosowanie narzędzi umożliwiających jednoczesne nagrywanie obrazu oraz dźwięku. Takie działanie mogłoby prowadzić do pozyskiwania informacji o charakterze szczególnym i naruszać prywatność osób, których dane dotyczą.

Nagrania mogą zawierać cechy szczególne osób monitorowanych, które ujawniają informacje o stanie zdrowia, pochodzenie rasowe, wyznanie, przynależność związkową. Jednakże dopóki nagrania nie są wykorzystywane w bibliotece do analizy tych cech, w szczególności automatycznych systemów dokonujących analizy nagrywanego obrazu, nie dochodzi do przetwarzania danych osobowych szczególnych kategorii, o których mowa w art. 9 ust. 1 RODO.

VII. Udostępnianie nagrań.

Jeżeli do biblioteki wpłynie wniosek o udostępnienie nagrania na potrzeby prowadzonego postępowania (policja, sąd, prokuratura, ABW, CBŚ, itp.), wówczas należy przechowywać nagranie do czasu prawomocnego zakończenia postępowania. W praktyce uzyskanie informacji o zakończeniu postępowania przez bibliotekę może nie być możliwe, ponieważ nie będąc stroną postępowania, nie jest uprawnionym do tego organem. Należy zatem przyjąć rozsądny okres czasu przechowywania udostępnionego fragmentu nagrania, a także określić oficjalnie ten okres w wewnętrznych procedurach, np. polityce ochrony danych osobowych.

Jeżeli do biblioteki wpływa wniosek od poszkodowanego o zabezpieczenie nagrania w związku z postępowaniem, w ramach, którego będzie ono udostępnione, należy poinformować go o tym, jak długo nagranie będzie przechowywane w związku ze złożonym wnioskiem. Istnieje ryzyko, że poszkodowany nie złoży zawiadomienia do organów ścigania (policji lub prokuratury) lub nie wystąpią one z wnioskiem o udostępnienie nagrania.

Każde udostępnienie nagrania musi być odnotowywane, ze wskazaniem za jaki okres nagranie zostało udostępniona oraz komu. Należy także przechowywać wnioski o udostępnienie, jako materiał stanowiący dowód, że udostępnienie nastąpiło zgodnie z uprawnieniem prawnie przysługującym wnioskującemu.

VIII. Klauzula informacyjna dla osób objętych monitoringiem wizyjnym.

W związku z wprowadzeniem monitoringu dyrektor biblioteki ma obowiązek oznaczyć miejsca monitorowane, a także przekazać osobom monitorowanym informacje, o których mowa w art. 13 ust. 1 i 2 RODO. Ze względu na szeroki zakres przekazywanych informacji, zalecane jest zastosowanie rozwiązania w postaci kaskadowego ich przekazywania. Pierwsze, niezbędne informacje, tzn. dane administratora danych, cel przetwarzania, czas przechowywania oraz kontakt w sprawach związanych z monitoringiem, przekazuje się na tablicach informacyjnych przed wejściem na teren oraz do budynku biblioteki. Tablica powinna odnosić do miejsca, w którym osoba monitorowana uzyska więcej niezbędnych informacji, np. strona internetowa, czytelnia.

IX. Powierzenie wideonadzoru agencji ochrony lub urzędowi gminy.

Jeżeli realizację obowiązków związanych z wiedonadzorem w bibliotece, w szczególności przechowywanie nagrań, w tym nadzór nad systemem monitoringu, udostępnianie nagrań, itp., wykonuje podmiot zewnętrzny, np. agencja ochrony lub urząd gminy, będzie pełnił on rolę podmiotu przetwarzającego dane na zlecenie biblioteki. Należy z tym podmiotem zawrzeć umowę powierzenia danych zgodnie z zasadami określonymi w art. 28 RODO.

9.8. Monitorowanie czasu i sposobu pracy.

Przepisy art. 22 Kodeksu pracy precyzują zakres danych, jakie może przetwarzać pracodawca w związku z realizacją procesu zatrudnienia. Przepisy zawarte w art. 22^3 dają pracodawcom możliwość monitorowania wykonania pracy pracowników celem jak najefektywniejszego wykorzystania czasu pracy. Monitoringiem mogą być objęte przede wszystkim elektroniczne skrzynki służbowe pracowników, ale także inne zasoby udostępniane przez pracodawcę do wykonywania pracy, np. dostęp sieci internetowej lub zastosowanie monitoringu GPS w służbowym samochodzie. Monitoring dostępu do sieci internetowej oraz monitoring samochodu służbowego pomaga określić, czy pracownicy wykorzystują te zasoby zgodnie z przeznaczeniem.

Pracodawca jest zobowiązany prowadzić monitoring pracowników zgodnie z czterema zasadami określonymi w prawie pracy:

a. Monitoring nie może naruszać tajemnicy korespondencji ani dóbr osobistych pracowników, także w przypadku, gdy służbowa skrzynka pocztowa służyła pracownikowi do wysyłania takich

wiadomości oraz w przypadku, gdy pracownik korzystał z prywatnej skrzynki pocztowej za pomocą sprzętu należącego do pracodawcy.

b. Przed wprowadzeniem monitoringu pracodawca musi określić zakres takiego monitoringu i zawrzeć go w regulaminie pracy, zbiorowym układzie pracy lub w obwieszczeniu oraz przekazać taką informację każdemu pracownikowi pisemnie.
c. Pracownicy muszą zostać poinformowani o planie zastosowania monitoringu przez pracodawcę co najmniej dwa tygodnie przed jego uruchomieniem.
d. Pracodawca musi zastosować oznaczenie za pomocą odpowiednich znaków (graficznych lub dźwiękowych) pomieszczenia i obszar podlegający monitoringowi, żeby pracownik mógł łatwo rozpoznać kiedy i w jakich sytuacjach jest monitorowany.

Jeśli dyrektor biblioteki chciałby zastosować monitoring poczty elektronicznej lub sposobu korzystania z Internetu, to konieczne jest zadośćuczynienie powyższym wymogom. Przede wszystkim należy poinformować pracowników o zakresie i celach wprowadzanego monitoringu drogą określoną w przepisach prawa oraz prawidłowo oznaczyć sprzęt komputerowy podlegający monitoringowi, np. za pomocą tapet wyświetlanych na pulpicie. Dobrym rozwiązaniem jest także zawarcie w wewnętrznych przepisach dotyczących ochrony danych osobowych zasad korzystania z poczty elektronicznej oraz sieci internetowej w taki sposób, by pracownik wiedział na co może sobie pozwolić korzystając z tychże zasobów. Wśród takich zapisów mogą być np. nakaz korzystania z poczty służbowej tylko do celów związanych ze świadczeniem pracy, zakazy rozsyłania łańcuszków czy odpowiadania na spam. Wskazane jest wprowadzić ograniczenie korzystania ze stron propagujących pornografię, rasizm, przemoc czy czyny zabronione, przy czym wachlarz ograniczeń może być dowolnie rozwijany w zależności od potrzeb pracodawcy.

Dobrą praktyką jest zawarcie w przepisach wewnętrznych zapisów o możliwości skorzystania z zasobów sieci internetowej do celów prywatnych, jeśli nie będzie to godziło w rzetelność i prawidłowe wykonanie obowiązków pracowniczych. Umożliwi to pracownikom okazyjne skorzystanie z zasobów pracodawcy i wpłynie korzystnie na efektywność pracy, gdyż pracownik będzie miał świadomość, że w losowych sytuacjach życiowych, które wymagają szybkiej reakcji, będzie mógł swoją sprawę załatwić bez konieczności łamania przepisów wewnętrznych i narażania się na karę.

Pracodawca kontrolując wykorzystanie zasobów internetowych oraz poczty elektronicznej musi mieć na względzie, że nie może pod żadnym pozorem naruszać tajemnicy korespondencji. Dotyczy to także przypadków, gdy pracownik wykorzystuje pocztę służbową do spraw prywatnych. W związku z tym w przypadku monitorowania zasobów internetowych należy sprawdzać wyłącznie strony, z jakich pracownik korzysta bez wglądu w treść wpisywanych haseł lub komentarzy (tzn. wystarczą adresy stron internetowych). Alternatywnym do monitoringu zasobów sieciowych rozwiązaniem może być zastosowanie oprogramowania (także antywirusowego), które selekcjonuje dostępność stron internetowych i umożliwia pracodawcy określenie, z jakich stron za pomocą sprzętu służbowego korzystać nie można. W przypadku poczty elektronicznej monitoring powinien obejmować np. ilość poczty przechodzącej przez skrzynkę, nagłówki i tytuły wiadomości czy formaty załączników.

Zautomatyzowanie procesu monitoringu poprzez zastosowanie odpowiedniego oprogramowania wydaje się być najbardziej efektywnym rozwiązaniem. Użyta może być do tego aplikacja monitorująca dostęp do udostępnianych zasobów (taką funkcję posiadają także niektóre programy antywirusowe). Pracodawca może za jej pomocą wygenerować raporty dotyczące odwiedzanych stron internetowych czy też może zostać zaalarmowanym o niewłaściwym korzystaniu z zasobów internetowych, gdy pracownik będzie do ich użycia chciał wykorzystać sprzęt służbowy. Jeśli chodzi o analizę poczty elektronicznej, dobrym rozwiązaniem byłoby generowanie raportów obejmujących przede wszystkim ruch na danych skrzynkach pocztowych, ale także takich, które, w miarę możliwości, chronią tajemnicę korespondencji, np. poprzez monitorowanie tytułów wiadomości oraz prze-

syłanych załączników. Przy wyborze oprogramowania należy także wziąć pod uwagę, czy dana aplikacja będzie dostosowana do używanego w jednostce sprzętu, by jej działanie nie zaburzało normalnego rytmu pracy pracownika np. poprzez znaczące obniżenie wydajności poszczególnych stacji roboczych.

Jeżeli zastosowano monitoring lokalizacji GPS w samochodzie służbowym, należy mieć na względzie, że taka usługa jest zazwyczaj świadczona przez firmę zewnętrzną, co wymaga zawarcia powierzenia danych osobowych.

9.9. Prowadzenie rekrutacji.

Prowadzenie procesu rekrutacji nowego pracownika wymaga wypełnienia przez administratora obowiązków wynikających z przepisów o ochronie danych osobowych oraz prawa praca. Dyrektor biblioteki od kandydata powinien pozyskiwać tylko niezbędne do procesu rekrutacji dane, których zakres został określony w art. 22^1 Kodeksu pracy, jak imiona, nazwiska, data urodzenia, wykształcenie, dane kontaktowe (telefon, e-mail, adres do korespondencji), przebieg zatrudnienia i kwalifikacje zawodowe. Jednakże w pewnych okolicznościach może być niezbędne pozyskanie dodatkowych informacji, np. jeżeli wynika to z przepisów szczególnych lub wymagań na konkretnym stanowisku pracy, np. znajomość języka angielskiego.

Na przetwarzanie tych danych nie jest konieczne uzyskanie zgody kandydata. Jako podstawę, zgodnie z art. 6 ust. 1 lit. c RODO, należy wskazać przepisy kodeksu pracy. Jednakże przyszły pracownik przekazuje także w swoim CV dodatkowe dane, jak zdjęcie, stan cywilny, zainteresowania, itp. Przekazanie tych danych powinno być dobrowolne i odbywać się za zgodą kandydata. Co do zasady, samo przesłanie aplikacji z nadmiarowymi danymi stanowi zgodę w rozumieniu art. 7 RODO, jednakże to na administratorze ciąży obowiązek wykazania, że faktycznie dane zostały przekazane, więc wskazane jest, aby w aplikacji została przez kandydata zamieszczona zgoda na przetwarzanie danych osobowych[19].

Dyrektor biblioteki może poszukiwać nie tylko pracowników, ale także wykonawców usług, którzy będą wspierać procesy biblioteczne na podstawie umowy cywilnoprawnej. W takim wypadku podstawą przetwarzania danych jest zawarcie umowy (w tym działania niezbędne przed zawarciem umowy), zgodnie z art. 6 ust. 1 lit. b RODO. W przypadku zleceniobiorców przepisy prawa pracy, ograniczające zakres danych, które można przetwarzać w związku z prowadzonym procesem rekrutacji, nie mają zastosowania. Dyrektor biblioteki określając wymagania i informacje, które musi przekazać mu wykonawca usługi, powinien kierować się więc zasadami minimalizacji i adekwatności danych do celu przetwarzania, zgodnie z art. 5 RODO, w szczególności ograniczyć wymagane dane do imion, nazwisk, danych kontaktowych, kwalifikacji, przebiegu zatrudnienia, doświadczenia, wykształcenia. Poszukiwanie wykonawcy nie można zakwalifikować jako rekrutację, jest to raczej spotkanie pomiędzy dwiema stronami umowy, tzn. zleceniobiorcy i zleceniodawcy, które te strony kształtują według własnych potrzeb.

Warto jeszcze w kontekście rekrutacji pracownika zwrócić uwagę na konieczność pozyskania od niego PESEL-u w związku ze skierowaniem na badania medycyny pracy. Powinien on być pozyskany przed zatrudnieniem, ale po zakończeniu procesu rekrutacji, czyli nie od wszystkich, ale od wybranego kandydata. Konieczność pozyskania PESEL-u wynika z przepisów rozporządzenia MZiOS w sprawie przeprowadzania badań lekarskich pracowników, zakresu profilaktycznej opieki zdrowotnej nad pracownikami oraz orzeczeń lekarskich wydawanych do celów przewidzianych w Kodeksie

[19] Przykładowy wzór zgody znajduje się w podrozdziale 9.13.

pracy. Oznacza to, że pozyskanie tej informacji jest obowiązkiem prawnym ciążącym na administratorze i nie wymaga zgody.

Poszukując nowych pracowników lub zleceniobiorców, dyrektor biblioteki jest zobligowany wypełnić wobec kandydatów obowiązek informacyjny z art. 13 ust. 1 i 2 RODO. Odpowiednia klauzula może być częścią ogłoszenia rekrutacyjnego / zapraszającego do współpracy lub przekazana zwrotnie, w odpowiedzi na przesłaną aplikację[20]. Należy zwrócić uwagę na sytuacje, w których CV zostało przekazane przez stronę trzecią, np. jednego z pracowników biblioteki. Wówczas także rodzi się obowiązek informacyjny, ale z art. 14 ust. 1 i 2 RODO. Rzetelne informowanie o zasadach przetwarzania danych, jest jednym z podstawowych obowiązków administratora wynikającym z przepisów RODO.

Po zakończeniu procesu rekrutacji, wszystkie dane kandydatów, tzn. aplikacje i wiadomości e-mail, powinny zostać zniszczone. W praktyce najczęściej ustala się ten okres na 3 do 6 miesięcy, od momentu zakończenia rekrutacji, co zazwyczaj jest związane z pozostawieniem sobie przez pracodawcę możliwości wykorzystania danych kandydatów, którzy nie zostali wybrani, w sytuacji, gdy zatrudniony kandydat nie spełni oczekiwań. Z drugiej strony rynek pracy jest dzisiaj na tyle dynamiczny, że może okazać się, że pozostawienie danych kandydatów mija się z celem, ponieważ we wskazanym okresie znajdą oni już inne zatrudnienie i nie będą zainteresowani. W takim wypadku usunięcie danych, powinno następować od razu po zakończeniu rekrutacji. Dyrektor biblioteki jest oczywiście uprawniony do przechowywania protokołu z procesu rekrutacji, który w przypadku wniesienia odwołania przez niewybranego kandydata, będzie stanowił punkt wyjścia do uzasadnienia wyboru.

Często zdarza się, że dyrektor biblioteki chce zatrzymać CV do przyszłych procesów rekrutacji. W takim wypadku, aby było to zgodne z wymaganiami przepisów RODO, jest zobligowany do uzyskania dodatkowej zgody kandydata[21], a także wypełnienia wobec niego obowiązku informacyjnego związanego z przetwarzaniem danych w tym celu. Warto podkreślić, że zgoda może zostać uzyskana poprzez odpowiedni zapis w CV, ale także w wiadomości e-mail lub na piśmie. Zgoda ustna także byłaby wiążąca, jednak administrator nie byłby w stanie wykazać, że faktycznie ją pozyskał.

Należy pamiętać, że obowiązkiem dyrektora biblioteki jest zapewnienie bezpiecznego środka komunikacji z przyszłym pracownikiem, który będzie przekazywał przyszłemu pracodawcy niezbędne informacje i dokumenty. W takim wypadku można zdecydować się na tradycyjne rozwiązanie, czyli osobistą wizytę przyszłego pracownika, który przekaże niezbędne dokumenty i wypełni niezbędne formularze lub zapewnić możliwość zaszyfrowania dokumentów przekazując procedurę szyfrowania oraz przekazania hasła.

9.10. Przetwarzanie danych w związku z przyznawaniem świadczeń z ZFŚS.

I. Wskazanie ADO i podstawy prawnej przetwarzania.

Pracodawca jest zobowiązany do utworzenia Zakładowego Funduszu Świadczeń Socjalnych, jeżeli zachodzą ustawowe przesłanki. Poza prawidłowym wykorzystywaniem środków zgromadzonych na rachunku funduszu zgodnym z ustawą o zakładowym funduszu świadczeń socjalnych i wewnętrz-

[20] Przykładowy wzór klauzuli informacyjnych znajduje się w podrozdziale 9.13.
[21] Przykładowy wzór zgody znajduje się w podrozdziale 9.13.

nym regulaminem, pracodawca zobligowany jest do zapewnienia obsługi technicznej, kadrowej i finansowej niezbędnej do funkcjonowania funduszu w zakładzie. Nieprawidłowości związane z administrowaniem środkami funduszu są obarczone odpowiedzialnością cywilną oraz karno-administracyjną.

Administratorem danych osobowych ZFŚS jest pracodawca (zakład pracy). Podstawę prawną przetwarzania danych osobowych zarówno pracowników, jak i członków ich rodzin prowadzących wspólnie gospodarstwo domowe, na potrzeby związane z działalnością socjalną stanowią przepisy art. 8 ustawy o ZFŚS w związku art. 6 ust. 1 pkt c RODO oraz art. 22 [1] Kodeksu pracy. Nie ma zastosowania art. 6 ust. 1 pkt a RODO w kwestii konieczności pobierania zgód na przetwarzanie danych osobowych, bowiem pozyskanie informacji jest konieczne do wypełnienia obowiązku prawnego ciążącego na administratorze. Podanie danych jest zatem wymogiem ustawowym a konsekwencją niepodania danych osobowych może być brak możliwości przyznania świadczeń z ZFŚS. Powołując się na wytyczne Poradnika dla pracodawców w przedmiotowej kwestii przetwarzanie danych osobowych koniecznych do skorzystania z usług i świadczeń finansowanych z funduszu nie może prowadzić do gromadzenia danych w zakresie szerszym, niż jest to konieczne dla realizacji celu, w jakim dane są pozyskiwane.

II. Postępowanie z wymaganymi i nadmiarowymi danymi osobowymi w ramach ZFŚS.

Przyznawanie świadczeń z funduszu jest uzależnione od kryterium socjalnego zgodnie z wymogami ustawy o zakładowym funduszu świadczeń socjalnych. Oznacza to, że sytuacja życiowa, rodzinna i materialna pracownika lub innej osoby uprawnionej do korzystania z Funduszu wymaga za każdym razem ponownej weryfikacji, czyli za każdym razem przetwarza się dane osobowe pracownika i członków jego rodziny w odniesieniu do konkretnego wniosku. Za źródła danych potwierdzających kryteria socjalne uważa się dokumenty zgromadzone w aktach osobowych pracownika, dokumenty dotyczące przebiegu ubezpieczenia społecznego, oświadczenia składane przez osoby uprawnione w celu udostępnienia pracodawcy danych osobowych, dokumenty przedłożone na żądanie pracodawcy w celu udokumentowania danych przekazanych przez osoby uprawnione (zaświadczenia, oświadczenia, inne dokumenty). Przetwarzanie danych musi odbywać się adekwatnie do celu oraz w zakresie wyłącznie niezbędnym do ustalenia aktualnej sytuacji pracownika, respektując tym samym zasadę minimalizacji danych (art. 5 ust. 1 lit c RODO). Zbieranie danych nadmiarowych związanych np. ze stanem zdrowia beneficjenta, których podanie w danym wniosku jest zbędne i nie ma wpływu np. na wysokość i przyznanie świadczenia, jest zakazane. Również zbieranie danych, które będą mogły zostać użyte w przyszłości nie ma podstaw prawnych i nie powinno być stosowane. Należy nadmienić, że niektóre ze świadczeń z ZFŚS mogą wiązać się przetwarzaniem danych osobowych szczególnej kategorii tzw. danych wrażliwych np. dotyczących stanu zdrowia. W myśl art. 9 ust. 2 lit. b RODO: „Przetwarzanie tego typu danych jest dozwolone, jeżeli jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa członkowskiego przewidującymi odpowiednie zabezpieczenia prawa podstawowych i interesów osoby, której dane dotyczą". Przedstawienie stosowanego dokumentu lub wypełnienie oświadczenia w celach weryfikacji jest zasadne i nie wymaga wyrażenia zgody na przetwarzanie tego typu danych osobowych. W sytuacji, kiedy pracownik nie będzie chciał złożyć stosownego oświadczenia, pracodawca nie będzie miał podstaw do wypłacenia świadczenia, o które ubiega się pracownik, ponieważ

przyznawanie ulgowych usług i świadczeń oraz wysokość dopłat z ZFŚS jest uzależnione od określonych w ustawie kryteriów. Wspomniane kwestie reguluje art. 8 ust.1a i 1d ustawy o ZFŚS:

„1a. Udostępnienie pracodawcy danych osobowych osoby uprawnionej do korzystania z Funduszu, w celu przyznania ulgowej usługi i świadczenia oraz dopłaty z Funduszu i ustalenia ich wysokości, następuje w formie oświadczenia. Pracodawca może żądać udokumentowania danych osobowych w zakresie niezbędnym do ich potwierdzenia. Potwierdzenie może odbywać się w szczególności na podstawie oświadczeń i zaświadczeń o sytuacji życiowej (w tym zdrowotnej), rodzinnej i materialnej osoby uprawnionej do korzystania z Funduszu.

1b. Pracodawca dokonuje przeglądu danych osobowych, o których mowa w ust. 1a, nie rzadziej niż raz w roku kalendarzowym w celu ustalenia niezbędności ich dalszego przechowywania. Pracodawca usuwa dane osobowe, których dalsze przechowywanie jest zbędne".

Wprowadzenie powyższych zapisów jest bardzo istotne, również z punktu widzenia zgromadzonej dotychczas dokumentacji w ramach ZFŚS. Okazanie dokumentów koniecznych do ustalenia sytuacji dochodowej rodziny, czy dokumentacji medycznej, gdy to jest niezbędne do przyznania prawa do świadczeń z ZFŚS jest uprawnieniem pracodawcy wynikającym z przepisów ustawy. W celu ograniczenia zakresu przetwarzanych danych, aby zapewnić zgodność z ustawą o ZFŚS oraz RODO, dokumenty wnioskodawca powinien przedstawiać komisji socjalnej do wglądu. Z przekazanych dokumentów komisja sporządza notatki służbowe, potwierdzające stan faktyczny. W notatce osoba upoważniona do jej sporządzenia potwierdza stan opisany we wniosku przez wnioskodawcę oraz podaje datę sporządzenia dokumentu i wskazuje organ, który go wydał. Należy ponadto zweryfikować posiadaną już dokumentację związaną z ZFSS pod kątem ochrony danych osobowych i przechowywanych kserokopii dokumentacji medycznej, którą powinno się zastąpić stosowną notatką służbową z faktu jej przedłożenia.

III. Upoważnianie pracowników i zapewnienie zobligowania do poufności.

Do przetwarzania danych osobowych pracowników, członków ich rodzin zarówno zwykłych jak i szczególnych kategorii, np. dotyczących zdrowia, o których mowa w art. 9 ust. 1 RODO, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania danych wydane przez ADO. Osoby dopuszczone do przetwarzania danych muszą zostać także zobowiązane do zachowania ich w tajemnicy. Do przetwarzania danych w bibliotece są upoważnieni przez ADO pracownicy, którzy są bezpośrednio odpowiedzialni za przetwarzanie danych, tacy jak pracownicy ds. kadrowych i płacowych, informatycy, księgowi oraz członkowie Komisji Zakładowego Funduszu Świadczeń Socjalnych.

Konieczność nadawania pisemnych upoważnień wynika z art. 8 ust. 1B ustawy o ZFŚS: „Do przetwarzania danych osobowych dotyczących zdrowia, o których mowa w art. 9 ust. 1 RODO, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania takich danych wydane przez pracodawcę. Osoby dopuszczone do przetwarzania takich danych są obowiązane do zachowania ich w tajemnicy". Upoważnienie pracodawca powinien wydać także do przetwarzania innych danych związanych z przyznawaniem świadczeń z Funduszu, pomimo że nie wynika to wprost z przepisów ustawy o ZFŚS, jednakże pozwoli to zapewnić rozliczalność przetwarzanych danych.

IV. Regulamin.

Biblioteka jako ADO ma za zadanie dopełnić obowiązku informacyjnego wobec osób, których dane są przetwarzane w ramach ZFŚS. Z uwagi na szeroki katalog osób uprawnionych do korzystania

z Funduszu do którego zalicza się pracowników, członków ich rodzin, emerytów i rencistów, byłych pracowników i inne osoby, którym pracodawca przyznał w regulaminie prawo korzystania ze świadczeń socjalnych finansowanych z funduszu, obowiązek ten powinien być spełniony w Regulaminie ZFŚS. W zależności od źródła uzyskania danych, tzn. bezpośrednio od wnioskodawcy lub pośrednio poprzez wnioskodawcę, zakres klauzuli informacyjnej będzie regulował odpowiednio art. 13 lub 14 RODO. Dopuszcza się formę informowania o zasadach przetwarzania danych w treści zapisów dotyczących przetwarzania danych osobowych w Regulaminie ZFŚŚ oraz w załącznikach do niego. Jedną z możliwości wypełnienia zapisów art. 14 RODO może być zobligowanie osób składających wniosek o ustalenie prawa do świadczeń z ZFŚŚ do przekazania osobom, których dane zostaną przez nich udostępnione we wniosku, wszystkich informacji dotyczących przetwarzania danych osobowych, aby miały możliwość sprawowania nadzoru nad swoimi danymi osobowymi, uwzględniając powyższe zobowiązanie w Regulaminie ZFŚŚ.

W obowiązującym w bibliotece regulaminie ZFŚS powinna znaleźć się kompleksowa informacja dotycząca przetwarzania danych osobowych. W treści należy wskazać ADO, osobę która pełni funkcję IOD, do którego można zwracać się w sprawach dotyczących przetwarzania danych osobowych, cel przetwarzania danych jakim jest przyznanie ulgowych usług i świadczeń oraz dopłat z ZFŚS. Niezwykle istotne jest określenie podstawy prawnej do przetwarzania danych oraz wskazanie okresu przechowywania danych i wszelkich przysługujących osobom uprawnionym i członkom rodzin praw z tytułu ich przetwarzania. Ważne jest także powiadomienie, że podanie danych jest dobrowolne, ale konsekwencją niepodania danych osobowych może być brak możliwości przyznania świadczeń z ZFŚS. Zalecane jest, aby w każdym wniosku o przyznanie świadczenia z ZFŚS zamieścić informację o tym kto jest administratorem danych i odnieść się do szczegółów związanych z przetwarzaniem danych osobowych zawartych w regulaminie ZFŚS.

9.11. Kasa zapomogowo pożyczkowa.

I. Podstawy prawne przetwarzania danych osobowych przez kasy zapomogowo-pożyczkowe.

Podstawę prawną do legalizacji działalności pracowniczych kas zapomogowo-pożyczkowych [PKZP] stanowią przepisy ustawy o związkach zawodowych. W art. 39 tejże ustawy, wskazano, że pracodawcy mogą tworzyć pracownicze kasy zapomogowo-pożyczkowe, których członkami mogą być pracownicy, emeryci lub renciści, bez względu na to, czy przynależą do związku zawodowego. Tworzenie i działalność kas reguluje również rozporządzenie w sprawie pracowniczych kas zapomogowo-pożyczkowych oraz spółdzielczych kas oszczędnościowo-kredytowych w zakładach pracy. Przynależność do PKZP jest dobrowolna. Przy przetwarzaniu danych osobowych jej członów ma zastosowanie art. 6 ust. 1 lit b RODO, tzn. podpisanie deklaracji członkowskiej i zaakceptowanie zasad działania kasy, oznacza umowę zawartą pomiędzy PKZP, a jej członkiem. Dane kontaktowe, jak numer telefonu czy adres e-mail mogą być przetwarzane na podstawie dobrowolnie wyrażonej zgody. W celach dowodowych powinno się gromadzić pisemne zgody na przetwarzanie danych kontaktowych, np. w deklaracji przystąpienia. Jeżeli członek kasy, nie będzie terminowo wywiązywał się ze zobowiązań, jak składki, czy spłata rat, to odzyskanie wierzytelności, będzie odbywać się na podstawie celów wynikających z prawnie uzasadnionych interesów realizowanych przez kasę (art. 6 ust. 1 lit. f RODO).

II. PKZP jako administrator danych osobowych.

Celem PKZP jest udzielanie jej członkom pomocy materialnej w formie nieoprocentowanych pożyczek długo- i krótkoterminowych oraz bezzwrotnych zapomóg na zasadach określonych w regulaminie. Organami PKZP są: walne zebranie członków oraz zarząd i komisja rewizyjna. Należy nadmienić, że kasa nie posiada osobowości prawnej. Tworzy odrębną strukturę organizacyjną mającą inne cele niż cel pracodawcy wobec pracownika i działa w oparciu o inne przepisy prawa. W związku z powyższym należy uznać, że w zakresie przetwarzania danych osobowych PKZP posiada status administratora danych. Zgodnie z art. 4 pkt 7 RODO: „Administrator oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych". PKZP jest ADO w stosunku do danych osobowych, które sama przetwarza i ponosi pełną odpowiedzialność za ochronę przetwarzanych danych. Największe kompetencje z reprezentowaniem kasy na zewnątrz włącznie, zgodnie z § 23 rozporządzenia o KZP ma zarząd. Zadaniem zarządu jest wdrożenie zasad skutecznej ochrony przetwarzanych przez kasę danych osobowych. Pracodawca jedynie udostępnia kasie pomieszczenie i sprzęt komputerowy na terenie swojej siedziby. Dodatkowo ze strony biblioteki na rzecz PKZP zagwarantowane jest miejsce na przechowywanie pieniędzy, transport pieniędzy z banku, prowadzenie księgowości, obsługa kasowa i prawna, dostarczanie druków i formularzy. Za pośrednictwem biblioteki dokonywane są również potrącenia wpisowego, wkładów miesięcznych i rat pożyczek. Jeżeli kasa jest ADO a biblioteka zobowiązana jest jedynie do zabezpieczenia działalności kasy tylko w określonych przypadkach, praktykowane jest, że kasa przyjmuje uchwałą do stosowania dokumentację przetwarzania danych osobowych, która została przyjęta w bibliotece, przy której działa kasa. W takim wypadku należy jednak dokonać wstępnej oceny przyjętych przez bibliotekę rozwiązań i przyjąć tylko te zasady, które faktycznie będą miały zastosowanie do działalności kasy, np. To gwarantuje spójność działań w zakresie ochrony danych osobowych zarówno po stronie pracodawcy jak i PKZP.

Należy podkreślić, że to PKZP ma obowiązki informacyjne wobec członków, wynikające z art. 13 ust. 1 i 2 RODO, które powinny być realizowane w momencie przystąpienia nowego członka do kasy, najlepiej poprzez zamieszczenie niezbędnych informacji w deklaracji członkowskiej. Można także pełną treść klauzuli zamieścić w regulaminie PKZP, a w deklaracji zamieścić jedynie pierwszą warstwę informacyjną z odniesieniem do regulaminu. W związku z przyznawaniem pożyczek przez PKZP, są przetwarzane także dane poręczycieli, wobec których także należy zrealizować obowiązek informacyjny, chociażby poprzez zamieszczenie odpowiednich zapisów w umowie pożyczki. Jest to dogodne rozwiązanie, ponieważ kasa będzie mogła wykazać, że wywiązała się z ciążących na niej obowiązków informacyjnych.

III. Możliwość powołania IOD przez PKZP.

Kasa jest autonomicznym administratorem danych w stosunku do swoich członków, jednak nie ma obowiązku wyznaczenia IOD wynikającego z kryteriów art. 37 ust. 1. RODO. Dodatkowo zarząd PKZP nie jest uprawniony do dowolnego dysponowania zgromadzonymi w kasie środkami, w szczególności w celu opłacania usług IOD. Jako ADO danych przetwarzanych w ramach kasy, ma obowiązek wykazać przestrzeganie przepisów RODO. Biblioteka przy której działa kasa jest zobowiązana jedynie do udzielenia nieodpłatnej pomocy. Warunki udzielania pomocy szczegółowo określa umowa zawarta z kasą. Nie ma bezpośredniego przeniesienia obowiązku wyznaczenia IOD przez PKZP nawet wówczas, gdy instytucja przy której działa kasa spełnia kryteria obligujące ją do wyznaczenia inspektora. Ewentualnym rozwiązaniem jest wskazanie w umowie, że biblioteka zapewnia nadzór swojego inspektora nad przetwarzaniem danych w kasie. Wówczas kasa jest zobligowana zapewnić

IOD odpowiednią niezależność oraz włączać go we wszystkie sprawy związane z przetwarzaniem danych. Dyrektor biblioteki może także na wniosek zarządu PKZP delegować własnego pracownika, który nie musi być członkiem kasy, który będzie wykonywał obowiązki zarządu w zakresie ochrony danych osobowych. Zarząd kasy powołuje wówczas delegowanego pracownika (pełnomocnika) kasy ds. ochrony danych osobowych, nadając mu stosowne upoważnienie.

9.12. Nagrywanie rozmów.

Głos osoby stanowi jej dane osobowe. Informacje, które bez nadzwyczajnego wysiłku, bez nieproporcjonalnie dużych nakładów dają się „powiązać" z określoną osobą, zwłaszcza przy wykorzystaniu łatwo osiągalnych źródeł powszechnie dostępnych, zasługują bowiem na zaliczenie ich do kategorii danych osobowych[22]. Za taką informację można z całą pewnością uznać głos danej osoby, który należy zaliczyć do kategorii danych osobowych zwykłych. Nagrywanie rozmów czyli nagrywanie głosu osób (np. nagrywanie przebiegu posiedzenia lub spotkania w celu sporządzenia protokołu, notatki lub sprawozdania, nagrywanie rozmowy telefonicznej) stanowi przetwarzanie danych osobowych.

Powyższe prowadzi do wniosku, że nagrywanie rozmów osób możliwe jest w przypadku spełnienia jednej z przesłanek stanowiących podstawę prawną przetwarzania danych określonych w art. 6 ust. 1 RODO. Należy zwrócić jednak uwagę, że głos osoby może w pewnych sytuacjach być uznany za dane biometryczne (zgodnie z art. 4 pkt 14 RODO dane biometryczne oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne). W przypadku uznania głosu osoby za dane biometryczne to znaczy, gdy głos osoby zostanie nagrany w celu ustalenia jej tożsamości, nagrywanie głosu tej osoby możliwe będzie w przypadku spełnienia jednej z przesłanek stanowiących podstawę prawną przetwarzania szczególnych kategorii danych osobowych określonych w art. 9 ust. 2 RODO.

Najczęstszą podstawą prawną nagrywania rozmów może być zgoda udzielona przez te osoby na nagrywanie rozmowy. Zgoda taka powinna udzielona przed rozpoczęciem nagrywania. W związku z powyższym osoby, których rozmowa będzie nagrywana powinny być o tym fakcie uprzedzone przed rozpoczęciem nagrywania. W przypadku braku zgody na nagrywanie głos danej osoby nie może być nagrywany.

Podstawę prawną nagrywania rozmów może stanowić także przepis prawa, w tym przepis prawa wewnętrznego, np. zarządzenie dyrektora biblioteki przewidujące obowiązek nagrywania przebiegu posiedzeń komisji przetargowej w celu sporządzenia protokołu z posiedzenia tej komisji.

Niezależnie od podstawy prawnej nagrywania rozmów administrator musi spełnić w stosunku do osoby (osób), których głos jest nagrywany obowiązek informacyjny, zgodnie z art. 13 RODO. Może nastąpić to przykładowo poprzez odczytanie informacji (klauzuli informacyjnej) na początku nagrywanej rozmowy lub też przekazanie takiej informacji w formie pisemnej (należy w tym przypadku pamiętać o konieczności uzyskania pisemnego potwierdzenia przekazania takiej informacji najlepiej w postaci podpisu osoby, której informacja została przekazana, na wydruku klauzuli). W przypadku odczytywania informacji należy odczytać ją w całości.

Jako, że głos osoby stanowi jej dane osobowe, również w przypadku nagranych rozmów, osobom, których głos został nagrany przysługują wynikające z RODO prawa związane z przetwarzaniem ich

[22] Zobacz Wyrok Naczelnego Sądu Administracyjnego z dnia 19 maja 2011 r., I OSK 1086/10, niepubl.

danych osobowych, w tym w szczególności prawo do wycofania zgody na przetwarzanie danych osobowych. Współczesne środki techniczne dają administratorom możliwość wypełnienia obowiązków związanych z prawami osób których dane dotyczą.

Brak jest przepisów powszechnie obowiązującego prawa określających zasady przechowywania, w tym okres przechowywania nagranych rozmów. Zasady te powinny zostać uregulowane przepisami wewnętrznymi obowiązującymi w danej bibliotece. Należy przy tym pamiętać, że nagrane rozmowy powinny zostać usunięte po ustaniu (zrealizowaniu) celu dla którego zostały nagrane.

Należy zwrócić uwagę, że nagrywanie rozmów bez zgody i wiedzy danej osoby (danych osób) stanowi nie tylko naruszenie przepisów o ochronie danych osobowych, ale także przepisów prawa karnego i prawa cywilnego. Zgodnie z art. 267 § 1 Kodeksu karnego „kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2". Na podstawie art. 267 § 3 Kodeksu karnego tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem". Oznacza to, że nieuprawnione nagrywanie rozmów osób trzecich lub nawet sam montaż lub posługiwanie się urządzeniami podsłuchowymi stanowi przestępstwo zagrożone sankcją karną. Niezależnie od powyższego nagrywanie rozmów danych osób bez ich zgody może stanowić naruszenie ich dóbr osobistych i stanowić podstawę do wniesienia pozwu przeciwko naruszającemu na podstawie art. 23 Kodeksu cywilnego. Potajemne nagrywanie rozmówcy narusza bowiem dobro osobiste w postaci swobody wypowiedzi oraz sferę prywatności rozmówcy[23].

9.13. Dobre praktyki, wytyczne i wskazówki.

I. Zgoda kandydata na przetwarzanie dodatkowych danych osobowych.

Prosimy o zamieszczenie dodatkowej klauzuli w treści CV:

Wyrażam zgodę na przetwarzanie moich danych osobowych, wykraczających poza wymagane przepisami kodeksu pracy, zawartych w dokumentach aplikacyjnych przez **[dane biblioteki i kontakt do niej]** w celu przeprowadzenia obecnego postępowania rekrutacyjnego Zostałem poinformowany, że podanie danych jest dobrowolne, a zgoda może być w dowolnym momencie wycofana

II. Zgoda na przyszłe procesy rekrutacji.

Prosimy o zamieszczenie dodatkowej klauzuli w treści CV, aby móc wykorzystywać CV do kolejnych procesów rekrutacji:

Dodatkowo zgadzam się na przetwarzanie moich danych osobowych przez **[dane biblioteki i kontakt do niej]** w celu prowadzenia przyszłych procesów rekrutacji.

[23] Zob. Wyrok Sądu Najwyższego z dnia 31 stycznia 2018 r., I CSK 292/17, niepubl.

III. Klauzula informacyjna dla kandydata.

5. Administratorem danych osobowych przetwarzanych w ramach procesu rekrutacji jest przez **[dane biblioteki i kontakt do niej]**
6. Kontakt do inspektora ochrony danych **podać adres e-mail i/lub telefon do IOD.**
7. Dane osobowe kandydatów będą przetwarzane w celu przeprowadzenia obecnego postępowania rekrutacyjnego na podstawie przepisów Kodeksu pracy oraz wyrażonej zgody (art. 6 ust. 1 lit. a i c RODO). Dane za zgodą kandydata mogą być także wykorzystywane do przyszłych procesów rekrutacji (art. 6 ust. 1 lit. a RODO). Od osoby wyłonionej w procesie rekrutacji administrator dodatkowo pozyska numer PESEL w celu wystawienia skierowania na badania wstępne, zgodnie z przepisami prawa pracy (art. 6 ust. 1 lit. c RODO).
8. Kandydatowi przysługuje prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.
9. Dane mogą być udostępnione podmiotom upoważnionym do tego na podstawie przepisów prawa, a także podmiotom świadczącym usługi w zakresie utrzymania poczty e-mail administratora**: [w szczególności.....]**
10. Dane kandydatów będą przetwarzanie **do czasu zakończenia** procesu rekrutacji, a w przypadku wyrażenia zgody na przetwarzanie w przyszłych procesach rekrutacji przez okres nie dłuższy niż **.....**
11. Kandydatowi przysługuje prawo dostępu do jego danych osobowych, żądania ich sprostowania, ograniczenia przetwarzania lub usunięcia. Wniesienie żądania usunięcia danych jest równoznaczne z rezygnacją z udziału w procesie rekrutacji.
12. Kandydatowi przysługuje prawo wniesienia skargi Prezesa Urzędu Ochrony Danych na niezgodne z prawem przetwarzanie jej danych osobowych.
13. Podanie danych jest dobrowolne, ale niezbędne do udziału w procesie rekrutacji.

10 ŚRODKI TECHNICZNE I ORGANIZACYJNE ZABEZPIECZENIA DANYCH OSOBOWYCH

10.1. Środki techniczne zabezpieczenia danych osobowych.

Dane osobowe przetwarzane w bibliotekach wymagają starannego zabezpieczenia. Zgodnie z RODO środki bezpieczeństwa dzielą się na techniczne i organizacyjne. Wśród środków technicznych oprócz klasycznych zabezpieczeń fizycznych coraz większe znaczenie mają zabezpieczenia danych przetwarzanych w cyberprzestrzeni. Warto podkreślić, iż w przepisach RODO dokonano szczegółowej regulacji w niektórych obszarach (np. przesłanki legalnego przetwarzania danych osobowych, zadania i status IOD), jednak w przypadku zabezpieczeń pozostawiono znaczącą autonomię ADO. Wynika to przede wszystkim z tego, że po wejściu w życie nowych uregulowań prawnych ochrona danych osobowych ma się opierać na analizie ryzyka i – w niektórych przypadkach – ocenie skutków dla ochrony danych. Przyjęto, że to ADO będzie w stanie najlepiej zdiagnozować obszary deficytowe i ocenić, jakie zabezpieczenia będą najbardziej efektywne. Jest to znacząca zmiana w stosunku do wymogu prawnego wynikającego z obecnie uznanego za uchylone rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Zgodnie z przepisami prawa obowiązującymi przed rozpoczęciem bezwzględnego obowiązywania RODO, każdy ADO musiał zastosować wskazane w rozporządzeniu zabezpieczenia, niezależnie od oceny ryzyka naruszenia poufności, integralności oraz dostępności danych zawartych w poszczególnych zbiorach.

Autonomia ADO w zakresie doboru środków bezpieczeństwa nie oznacza jednak, że w RODO nie odniesiono się do konkretnych rozwiązań. W art. 32 ust. 1 RODO wskazano:

- pseudonimizację i szyfrowanie danych osobowych,
- zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Warto zwrócić uwagę, że wszystkie te działania zostały wskazane w dość dużym stopniu uogólnienia, jednak stanowią wyraźną sugestię, na co powinno się zwrócić szczególną uwagę podczas zabezpieczenia danych. Pojęcie, które wymaga wyjaśnienia to „pseudonimizacja". Zgodnie z definicją zawartą w art. 4 RODO oznacza ono „przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do

zidentyfikowania osobie fizycznej". Natomiast przykłady mechanizmów szyfrowania danych osobowych i innych działań w systemie informatycznym zostały przedstawione w podrozdziale 10.2.

Informacje na temat zabezpieczenia danych osobowych znajdują się także w preambule RODO. Wskazano tam m.in., że należy zapewnić odpowiednie środki umożliwiające zgłaszanie naruszeń bezpieczeństwa danych osobowych do właściwego organu nadzorczego. W preambule odniesiono się także do kwestii korzystania z dostępnej wiedzy w wymiarze interdyscyplinarnym i osiągnięć techniki w zakresie kreowania środków bezpieczeństwa danych. W przypadku bibliotek warto zastosować różnorodne rozwiązania w zależności od zakresu i skali przetwarzanych danych osobowych, jak również możliwości organizacyjnych i finansowych. W przypadku spodziewanej kontroli lub audytu wewnętrznego lub zewnętrznego, warto zweryfikować zastosowane zabezpieczenia pod kątem wskazanych wcześniej informacji zawartych w art. 32 ust. 1 RODO.

Inne środki techniczne służące do zabezpieczenia danych osobowych to m.in.:

- gaśnice, koce gaśnicze przeciwpożarowe – to zabezpieczenia, które z pozoru nie są związane z ochroną danych osobowych, jednak w sytuacjach kryzysowych mogą przyczynić się do uniknięcia utraty danych; szczególnie istotna jest, aby znajdowały się w serwerowni i pomieszczeniach służących jako archiwa z dokumentami;
- czujniki dymu – umożliwiają prewencję zagrożeń w zakresie pożarów,
- odpowiednie szafy – materiał z jakiego zostały wykonane oraz rodzaj zamka powinny być dostosowane do zakresu danych osobowych, jakie są w nich przechowywane (szczególną uwagę warto zwrócić na dokumenty kadrowe i dokumenty zawierające dane osobowe czytelników); szafy nie muszą być fabrycznie nowe, ani atrakcyjne wizualnie, w przypadku braku wystarczających środków finansowych warto rozważyć zamontowanie zamka w już używanej szafie,
- odpowiednie ustawienie mebli – należy ustawiać meble w sposób uniemożliwiający dostęp osób postronnych i zwrócić uwagę na ustawienie monitorów komputera (warto unikać ustawiania monitora przy lustrze lub w sposób umożliwiający odczytanie wyświetlanych informacji przez osoby postronne,
- profesjonalna niszczarka lub umowa z firmą niszczącą dokumenty – w bibliotece powinna znajdować się przynajmniej jedna niszczarka (warto rozważyć zakup niszczarki zgodnej z normą DIN 66399); alternatywą jest podpisanie umowy z firmą niszczącą dokumenty, wymaga to jednak znalezienia rzetelnego podmiotu i podpisania umowy powierzenia danych osobowych, a dokumenty przeznaczone do zniszczenia powinny być przechowywane w specjalnym pojemniku,
- filtry prywatyzujące – ich umieszczenie na monitorach komputerów umożliwia ograniczenie dostępu osób postronnych (rozwiązanie to jest szczególnie funkcjonalne w przypadku braku możliwości ustawienia monitora w sposób uniemożliwiający odczytanie danych przez osoby postronne); za pomocą filtra możliwe jest ograniczenie widoczności nawet pod kątem 15 stopni,
- unikanie pozostawiania kluczy w drzwiach – niedopuszczalne jest zostawianie kluczy w drzwiach, nie tylko ze względu na zagrożenie dostępu osób postronnych do danych osobowych, ale również ze względu na bezpieczeństwo osób pracujących w pomieszczeniach,
- inne rozwiązania związane z innowacyjnym podejściem niektórych producentów zabezpieczeń, np. rolki maskujące, które swoim wyglądem przypominają pieczątki, jednak zamiast danych na pieczątce pojawia się szereg liter i cyfr w żaden sposób nie powiązanych ze sobą, co umożliwia zamazanie danych osobowych, np. na kopercie lub dokumencie.

10.2. Bezpieczeństwo teleinformatyczne i bezpieczeństwo danych osobowych w cyberprzestrzeni.

I. Cyberprzestrzeń jako przestrzeń przetwarzania informacji w systemach teleinformatycznych w tym ograniczenia jawności informacji w cyberprzestrzeni.

W związku z postępującą informatyzacją bibliotek i podejmowaniem działań z wykorzystaniem sieci Internet warto dbać o bezpieczeństwo danych osobowych w cyberprzetrzeni i systematycznie ten obszar rozwijać. Znanych jest wiele przypadków utraty ważnych informacji, kradzieży danych czy ujawnienia ich, w tym danych osobowych. Cyberprzestrzeń stała się obszarem działania instytucji sektora publicznego oraz organizacji sektora prywatnego, równie ważnym jak płaszczyzna materialna. Obszary te (materialny i wirtualny) traktowane są jako powiązane ze sobą i niezbędne do funkcjonowania we współczesnym świecie.

Wraz z upływem czasu i rozwojem technologii definicja cyberprzestrzeni zmieniała się wielokrotnie. Ogólnie przyjmuje się, że cyberprzestrzeń jest to iluzja świata rzeczywistego stworzona za pomocą narzędzi teleinformatycznych. Czyli jest to przestrzeń wirtualna, w której połączone w sieć urządzenia komunikują się między sobą, ułatwiając wymianę, gromadzenie i udostępnianie informacji. Przestrzeń ta służy do komunikowania się ludzi oraz umożliwia komunikację między człowiekiem i komputerem. Obecnie najczęściej do łączenia w sieć urządzeń służy Internet. Podstawowe elementy tego środowiska to: rozległość (zasięg), spajanie, wielkość bazy danych (suma danych zawartych w systemach danych), złożoność (różne systemy danych, pliki, aplikacje, procesy czy strony internetowe) oraz brak możliwości odniesienia do fizycznych wymiarów (przestrzeń wirtualna, nieistniejąca fizycznie). Jest to logicznie wyodrębniony obszar związany z cyfrową domeną przetwarzania i wymiany informacji. To obszar równoległego środowiska, w którym środowisko naturalne, realne i fizyczne zastąpione jest środowiskiem programowym. Cyberprzestrzeń stała się obszarem działalności firm i innych podmiotów, w których narzędzia informatyczne to element zarządzania operacyjnego.

W instytucjach i firmach informacja stanowi wsparcie w zakresie realizacji podejmowanych działań poprzez jej gromadzenie lub komunikację. W wielu przypadkach jest też obszarem głównej działalności organizacji. W bibliotekach poprzez przenoszenie posiadanych zasobów do postaci cyfrowej jest i będzie obszarem pomocniczym. W zakresie poziomu komunikacji z biblioteką jest to poziom równoległy z kontaktem bezpośrednim. Cyberprzestrzeń jest ogólnie dostępna, a dostęp do jej zasobów może zostać ograniczony.

W zależności od poziomu organizacyjnego podmiotu, ograniczenie takie może wynikać z różnych przesłanek. Inne przesłanki będą odpowiadały za takie ograniczenia na poziomie państwowym, inne korporacyjnym, jeszcze inne na poziomie przedsiębiorstw. Dla przykładu na poziomie państwa takimi przesłankami będą stabilność gospodarcza i ekonomiczna państwa oraz jego obrona i bezpieczeństwo. Na poziomie podmiotów gospodarczych będzie to zdolność do dostosowywania się do nowych wyzwań ekonomicznych i technologicznych oraz tworzenia skutecznych rozwiązań, by tym wyzwaniom sprostać.

Istnieje wiele przykładów ograniczeń jawności informacji w cyberprzestrzeni. Do takich ograniczeń zaliczyć można ochronę informacji niejawnych, ochronę tajemnicy przedsiębiorstwa, ochronę tajemnic ustawowo chronionych, ochronę prywatności oraz ochronę danych osobowych. Ochrona informacji niejawnych oznacza chronienie informacji, której nieuprawnione ujawnienie (nawet w trakcie jej opracowywania oraz niezależnie od formy i sposobu jej wyrażania) spowodowałoby lub mogłoby spowodować szkody dla właściciela informacji albo byłoby z punktu widzenia jego interesów

niekorzystne. Poprzez poufność wskazano obszar, w którym informacje te nie powinny być udostępniane lub ujawniane nieuprawnionym osobom, procesom lub innym podmiotom. Poprzez poufność zapewniono także środki proceduralne i techniczne, takie jak wydzielone pomieszczenia, szyfrowanie i kontrola dostępu.

Istotne znaczenie ma także ochrona prywatności. W przypadku bibliotek oznacza ona zarówno ochronę prywatności pracowników, jak również osób korzystających z usług biblioteki. Polega ona na chronieniu zdolności jednostki lub grupy osób do utrzymania swych danych oraz osobistych zwyczajów i zachowań nieujawnionych publicznie w prywatności. Prawo do prywatności określane jest jako fundamentalne i podstawowe prawo człowieka. Jego ważność widać po unormowaniu jego ochrony w normach nie tylko krajowych, ale i międzynarodowych. Odniesiono się do tego zagadnienia m.in. w Powszechnej Deklaracja Praw Człowieka, Międzynarodowym Pakcie Praw Obywatelskich i Politycznych, Europejskiej Konwencji Praw Człowieka, Karcie Praw Podstawowych UE oraz orzecznictwie Europejskiego Trybunału Praw Człowieka. Na gruncie prawa polskiego prawo do prywatności unormowane zostało w Konstytucji RP. Do przepisów Konstytucji RP dotyczących prywatności odnoszą się przepisy Kodeksu cywilnego, Kodeksu karnego i Kodeksu postępowania karnego dotyczące jej ochrony. Takie podejście organów państwa wskazuje negatywny i pozytywny wymiar uregulowań w tym zakresie. Negatywny dotyczy zakazu podejmowania działań i przyjmowania uregulowań prawnych, które reglamentowałyby sferę prywatności, w sposób pozbawiony konstytucyjnego uzasadnienia. Pozytywny wymiar dotyczy nakazu podejmowania działań, mających na celu ochronę jednostki przed nieuzasadnionymi naruszeniami jej prywatności. Zagrożenia dla prawa do prywatności we współczesnym świecie można dostrzec na kilku płaszczyznach, m.in. w działaniach służb i administracji państwowej, zbieraniu danych przez firmy, nadzorowi nad pracownikami, Internetem i telefonią komórkową, monitoringowi wizyjnemu oraz rozwojowi biometrii. Państwa rozbudowują instrumenty prawne ochrony prywatności, lecz jednocześnie tworzą normy prawne pozwalające na ingerencję w tę ochronę. Częścią tej materii jest ochrona danych osobowych.

II. Cyberbezpieczeństwo.

Z pojęciem cyberprzestrzeni nierozerwalnie wiąże się pojęcie cyberbezpieczeństwa. Pojęcie to obejmuje rozwiązania służące bezpieczeństwu teleinformatycznemu, w tym bezpieczeństwu danych osobowych w cyberprzestrzeni. Cyberbezpieczeństwo powinno znaleźć się na początku listy priorytetów wszystkich podmiotów mających styczność z cyberprzestrzenią oraz wszystkich osób za to bezpieczeństwo odpowiedzialnych. Cyberbezpieczeństwo to też bezpieczeństwo infrastruktury, począwszy od pojedynczego sprzętu komputerowego czy telefonicznego po całościowo rozumianą infrastrukturę teleinformatyczną, w tym infrastrukturę krytyczną. Do szerokiego spektrum zagrożeń związanych z funkcjonowaniem w cyberprzestrzeni należą: dezinformacja, trolling, działania mające na celu naruszenie dobrego imienia podmiotu oraz podważenie jego wiarygodności, zakłócające realizację istotnych zadań. Do najczęściej występujących zagrożeń w cyberprzestrzeni należą: ataki z użyciem szkodliwego oprogramowania (malware, wirusy, robaki, trojany, keyloggery, itp.), kradzieże tożsamości, kradzieże, wyłudzenia, modyfikacje bądź niszczenie danych, blokowanie dostępu do usług, spam (niechciane lub niepotrzebne wiadomości elektroniczne), ataki socjotechniczne (np. phishing, czyli wyłudzanie poufnych informacji przez podszywanie się pod inną osobę lub instytucję).

Istotne znaczenie mają także wiadomości e-mail zawierające w załączniku „fałszywą" fakturę, nakaz zapłaty albo informację o przesyłce kurierskiej. Najczęstszymi przyczynami cyberataków są działania (w tym błędy) obecnych i byłych pracowników. W celu zapobiegania takim negatywnym zjawiskom warto szkolić i uświadamiać pracowników. Podnoszenie kwalifikacji pozwala na zmniej-

szenie liczby incydentów, a w wypadku ich wystąpienia, na szybką reakcję, dzięki czemu ograniczane są ich negatywne skutki. Jednocześnie warto zabezpieczać sprzęt w bibliotece oraz ograniczyć dostęp do niego z zewnątrz. Dobrą i zalecaną praktyką jest wprowadzenie separacji sieci wewnętrznej (bibliotecznej) od zasobów zewnętrznych. Sieci LAN łatwo można spenetrować, poprzez dostęp do niezabezpieczonych urządzeń, takich jak: routery WiFi, komputery, laptopy, kamery, drukarki, itd. Za pośrednictwem sieci przekazuje się często dane poufne i kluczowe, tzn. w wiadomościach e-mail, w systemach bibliotecznych, systemach kadrowych, systemach bankowych, itp. Takie dane wymagają środków bezpieczeństwa w postaci ograniczeń dostępu. Można tego dokonać poprzez separację ruchu między określonymi grupami portów lub grupy określonych adresów fizycznych MAC. Jeszcze inny rodzaj separacji sieci określa się na podstawie wykorzystywanej przez użytkowników aplikacji lub kryteriów wybranych przez użytkownika, a zdefiniowanych w formacie ramki danego protokołu sieciowego. Są to sieci wirtualne określone na podstawie własnych kryteriów użytkownika i na podstawie parametrów przekazanych przez serwer uwierzytelniania. Dostęp z zewnątrz do takiej odseparowanej sieci jest ograniczony, natomiast dostęp do zasobów zewnętrznych jest możliwy i nie ma potrzeby z niego rezygnować. Dostęp do takiej sieci uzyskujemy poprzez VPN czyli tzw. tunelowanie. Jest to tunel przez który płynie ruch w ramach sieci prywatnej pomiędzy klientami końcowymi za pośrednictwem publicznej sieci w taki sposób, że węzły tej sieci nie widzą przesyłanych w ten sposób danych (dane są zabezpieczone kryptograficznie). Dodatkowo można kompresować lub szyfrować przesyłane dane w celu zapewnienia większego poziomu bezpieczeństwa. VPN przekierowuje ruch internetowy do specjalnie skonfigurowanego serwera, ukrywając adres użytkownika i szyfrując wysyłane i odbierane dane. Zaszyfrowane dane są niemożliwe do odczytania przez podmioty, które je przechwycą. Dostęp do sieci Internet przez VPN można zrozumieć za pomocą metafory wysyłania pocztą tradycyjną paczki w pudełku. Nikt nie może się dowiedzieć, co znajduje się w pudełku, do momentu jego otwarcia, w związku z tym stosowanie tego rozwiązania wraz z wydzielaniem sieci wewnętrznych na podsieci, powinno być standardem stosowanym w każdej bibliotece, który pozwoli zapewnić zgodność zastosowanych środków technicznych z przepisami art. 32 RODO.

Natomiast w zakresie ograniczenia dostępu nośników (pendrive, zewnętrzne dyski, CD, DVD) należy zwrócić uwagę na wyłączenie funkcji automatycznego uruchamiania (ang. autorun) dla wszystkich nośników, a w uzasadnionych przypadkach ograniczenie możliwości dowolnego podłączania pamięci USB do stanowisk komputerowych, tzn. możliwe będzie podłączenie tylko uwierzytelnionego wcześniej przez informatyka urządzenia. Istotne znaczenie ma także skanowanie programem antywirusowym zewnętrznych nośników danych przed każdym użyciem (najlepiej ustawione jako domyśle, aby użytkownik nie musiał podejmować dodatkowego działania) oraz ograniczenie do niezbędnego minimum wymiany danych za pośrednictwem zewnętrznych nośników (zwłaszcza typu pendrive), a w szczególności pomiędzy komputerami podłączonymi do sieci Internet, a stanowiskami od niej odseparowanymi. Jeżeli niezbędne jest zapewnienie wymiany informacji pomiędzy użytkownikami, należy rozważyć wdrożenie wewnętrznego serwera plików, najlepiej niedostępnego poza biblioteką lub z ograniczoną możliwością dostępu, np. przez VPN.

Kolejnymi ważnymi czynnościami jest zmiana ustawień fabrycznych sprzętu i dopasowanie jego ustawień do naszych preferencji. Często użytkownik nie ma świadomości jakie są implikacje podłączania coraz większej liczby urządzeń do sieci i w związku z tym nie zmienia domyślnych ustawień i nie aktualizuje ich oprogramowania. Może to być przyczyna włamania do sieci (np. błędna konfiguracja zapory sieciowej). Podczas instalacji aplikacji użytkownik zawsze jest proszony o zaakceptowanie warunków świadczenia usługi. Zdarza się jednak, że użytkownicy nie czytają pojawiających się komunikatów, akceptując ustawienia fabryczne, które nie stanowią odpowiedniego zabezpieczenia danych. Dlatego warto obejrzeć dokładnie listę uprawnień, o akceptację których użytkownik jest proszony, a instalowanie nowego oprogramowania powinno być dokonywane tylko i wyłącznie przez

administratora. Użytkownik powinien mieć ograniczone uprawnienia, które nie dają mu możliwości instalowania oprogramowania ani zmiany ustawień już zainstalowanego oprogramowania, np. wyłączenia antywirusa, aktualizacji lub zapory systemu.

Należy zwrócić uwagę również na nowe zagrożenie. Istnieje wiele tzw. „urządzeń Internetu rzeczy", podłączonych do sieci zarówno w biurach, jak i w domach. Mają one stały dostęp do sieci, co oznacza, że niezależnie w jaki sposób użytkownik próbuje zabezpieczyć swój komputer, cyberprzestępca zawsze może użyć tzw. 'backdoor' i zaatakować. Atak polega na nielegalnym dostępie do sesji użytkownika i przejęciu nad nią kontroli. Po przejęciu kontroli nad urządzeniem IoT, atakujący widzi wszystkie pakiety wysyłane przez serwer i użytkownika. Wśród rozwiązań, które mogą przyczynić się do zwiększenia bezpieczeństwa biblioteki w cyberprzestrzeni warto wskazać:

- zobowiązanie pracowników do zachowania w tajemnicy wszelkich informacji chronionych, w tym danych osobowych,
- zwiększanie świadomości w zakresie bezpieczeństwa danych (szkolenia),
- ustawienie monitorów w sposób uniemożliwiający wgląd osobom postronnym,
- założenie filtrów na monitory,
- przechowywanie kopii zapasowych w innym pomieszczeniu i/lub poza siedzibą firmy,
- szyfrowanie danych,
- określenie zakresu przetwarzania danych osobowych przez pracownika,
- obowiązek noszenia identyfikatorów służbowych (ograniczenie dostępu),
- niszczenie urządzeń, dysków i innych nośników w sposób uniemożliwiający odzyskanie danych,
- bieżące usuwanie zbędnych plików/wiadomości,
- ochrona urządzeń mobilnych używanych w bibliotece.

Bezpieczny komputer powinien mieć zainstalowane oprogramowanie 'security' w tym program antywirusowy i firewall (zapora systemowa). Warto pamiętać, że bezpieczne jest pobieranie aplikacji tylko z zaufanych źródeł. Istotne jest także usuwanie nieużywanych aplikacji. Nie należy podłączać urządzeń do ogólnodostępnych sieci Wi-Fi (szczególnie poza siedzibą biblioteki) lub Bluetooth. Dostęp z zewnątrz do wewnętrznego dysku sieciowego powinien odbywać się zawsze z wykorzystaniem VPN. Należy także zasłaniać kamerę, w którą może być wyposażony komputer i nie wolno zostawiać bez nadzoru niezablokowanego komputera. Nie wolno kopiować dokumentów identyfikacyjnych oraz kart kredytowych i nie należy umieszczać ich w mediach społecznościowych.

Jeżeli w bibliotece używany jest dysk sieciowy, warto umieścić go w bezpiecznym, separowanym segmencie sieci. Jeżeli w bibliotece funkcjonuje system monitoringu lub kontroli dostępu, należy zawsze ograniczać do niego dostęp. Warto także szyfrować przenośne nośniki danych. Istotne znaczenie ma także niepodłączanie do służbowej sieci komputerowej prywatnych urządzeń, otrzymanych lub znalezionych nośników pamięci oraz płyt CD/DVD, gdyż mogą być zainfekowane złośliwym oprogramowaniem.

Jednocześnie pracownicy biblioteki powinni ograniczyć komunikację pomiędzy urządzeniami tylko do połączeń, które są im znane. Warto także systematycznie poszerzać wiedzę na temat cyberbezpieczeństwa, np. poprzez czytanie o najnowszych podatnościach na stronach fachowych oraz sprawdzanie potencjalnych następstw aktualizacji. Równie istotne jest zachowanie ostrożności przy odbieraniu wiadomości e-mail, klikaniu w przesłane linki i otwieraniu załączników od nieznanych osób lub firm, a także przy przekazywaniu informacji nieznanym osobom, co do których nie ma pewności (bądź możliwości weryfikacji), czy są tymi, za kogo się podają. Znaczący wpływ na bezpieczeństwo ma także zgłaszanie do IOD oraz informatyka wszystkich podejrzanych i nietypowych sytuacji związanych ze sprzętem lub oprogramowaniem oraz otrzymanymi wiadomościami e-mail.

Bardzo ważna jest polityka haseł. Od ich odporności na złamanie zależy bezpieczeństwo danych

posiadanych w zasobach biblioteki. Nawet najlepszy system ochrony może być nieskuteczny, jeśli hasło będzie podatne na złamanie. Niektórzy pracownicy bibliotek nie znajdują czasu na zapoznanie się z zasadami dotyczącymi haseł, jednak warto je poznać i dzięki temu zadbać o bezpieczeństwo w sieci. Należy stosować niewystępujące w słowniku, unikatowe hasła, nie krótsze niż 8 znaków (najlepiej dłuższe niż 8 znaków) zawierające duże i małe litery, znaki specjalne i cyfry. Należy unikać haseł, wykorzystujących popularne frazy, slang, nazwy miejsc czy imiona. Hasła powinny być długie, ale łatwe do zapamiętania. Należy unikać haseł składających się z sąsiadujących na klawiaturze klawiszy. Na pierwszy rzut oka wyglądają one skomplikowanie, jednak w rzeczywistości są to wpisane kolejno przyciski na klawiaturze. Stanowi to jeden z najczęściej popełnianych błędów przy tworzeniu haseł. Należy je zmieniać w przypadku pojawienia się jakiejkolwiek oznaki zwiastującej włamanie. Istotne jest także nieujawnianie haseł nawet najbardziej zaufanym współpracownikom, niezapisywanie haseł i loginów na publicznych komputerach, ani na kartkach lub tablicach przy stanowisku komputerowym. Wpisując hasło warto upewnić się, że nikt nie widzi jaka jest jego treść. Nie należy także używać tych samych haseł do różnych kont, ponieważ w przypadku utraty poufności danych do logowania do jednego systemu, konieczna będzie zmiana haseł do wszystkich. Jeżeli istnieje taka możliwość, zawsze warto rozważyć również weryfikację dwuetapową (np. hasło i kod z SMS-a czy aplikacji). Dane do logowania nie powinny być ujawniane innym pracownikom. Jest to istotne wyzwanie dla cyberbezpieczeństwa w bibliotece, gdyż w sezonie urlopowym, trzeba zapewnić możliwość zastępowania się przez pracowników, bez konieczności przekazywania dostępu do systemów i plików. Podobnie logowanie do systemów powinno odbywać się z wykorzystaniem indywidualnych loginów oraz haseł, tak aby zapewnić rozliczalność czynności wykonywanych na danych w tych systemach. Przedstawione informacje prowadzą do konkluzji, iż zasady dotyczące haseł nie są skomplikowane i łatwo wprowadzić je w życie. Dodatkowo można je uprościć dzięki korzystaniu z programu do generowania, przechowywania i zarządzania hasłami.

10.3. Środki organizacyjne zabezpieczenia danych osobowych.

Jako osobne zagadnienie należy potraktować organizacyjne środki zabezpieczenia danych osobowych. Są one związane przede wszystkim ze środowiskiem wewnętrznym, rozumianym jako kadra kierownicza oraz pracownicy biblioteki i występujące między nimi interakcje. Pierwszy okres obowiązywania RODO stanowi wykładnik, a w zasadzie potwierdzenie przypuszczeń specjalistów w zakresie ochrony danych osobowych, że jedną z najistotniejszych przyczyn naruszeń bezpieczeństwa danych są błędy ludzkie. W większości przypadków są one nieumyślne i wynikają z braku wiedzy, bądź też z niedopatrzenia. Warto podkreślić, że błędy ludzkie są niemożliwe do całkowitego wyeliminowania. Można jednak podjąć środki organizacyjne, które zmniejszają prawdopodobieństwo ich wystąpienia. Kluczowa w tym zakresie jest rola dyrekcji biblioteki. Podejście pracowników biblioteki do szerokiego spektrum zagadnień związanych z ochroną danych osobowych w dużej mierze zależy od tego, jaki jest stosunek kierownika jednostki do tego obszaru. Warto więc przede wszystkim przypominać pracownikom o znaczeniu ochrony danych osobowych i stosowania przepisów RODO dla funkcjonowania całej instytucji. Zgodnie z definicją zawartą w art. 4 RODO, administrator ustala cele i sposoby przetwarzania danych osobowych. Pomimo tego, że strategiczne decyzje dotyczące funkcjonowania biblioteki podejmuje dyrekcja, bardzo wiele decyzji krótkoterminowych dotyczących codziennych działań w bibliotece podejmują także pracownicy. Pracownicy muszą więc zdawać sobie sprawę, że ADO to nie dyrekcja, lecz cała biblioteka, a ich działania i decyzje mają istotne znaczenie dla bezpieczeństwa danych osobowych – ich własnych, współpracowników, a także osób korzystających z biblioteki.

Pracownicy mogą zdobywać informacje na temat stosowania w praktyce przepisów RODO podczas szkoleń wewnętrznych i zewnętrznych, jak również poprzez czytanie artykułów specjalistycznych i innych opracowań dotyczących ochrony danych osobowych. W tym przypadku warto pamiętać, żeby szkolenia i zakupione opracowania odnosiły się do problematyki stosowania przepisów RODO w bibliotekach, ponieważ tylko wtedy będą wartościowe dla pracowników biblioteki. Warto podkreślić, że podstawowym źródłem informacji na temat ochrony danych osobowych dla pracowników powinny być procedury wewnętrzne (opisana szczegółowo w rozdziale VI niniejszego Kodeksu dokumentacja ochrony danych osobowych). W tym przypadku również bardzo istotna jest rola kadry kierowniczej w zakresie uświadomienia pracownikom jak bardzo istotne jest zapoznanie się z dokumentacją.

Osobną kwestią, również związaną z pracownikami biblioteki jest nadawanie im upoważnień do przetwarzania danych osobowych. Z przepisów RODO nie wynika bezpośrednio, że taka czynność ma charakter obligatoryjny. Trudno jednak w inny sposób zapewnić rozliczalność danych osobowych w kontekście tego, kto ma dostęp do poszczególnych ich zbiorów oraz do systemów informatycznych. Coraz częściej stosowaną praktyką jest nadawanie upoważnień dla pracowników przez IOD, jako osoby zajmującej się w bibliotece ochroną danych osobowych. Nawet jeśli IOD został upoważniony przez dyrekcję do nadawania takich uprawnień, nie jest to rozwiązanie, które zasługuje na rekomendację. W takiej sytuacji tworzy się bowiem pozory, że IOD to ADO. Zakres zadań IOD jest natomiast zupełnie inny i nie ma w nim elementów związanych z zarządzaniem. IOD może natomiast wspierać dyrekcję w procesie nadawania uprawnień, jednak oficjalne dokumenty w tym zakresie powinien zatwierdzać swoim podpisem dyrektor biblioteki. Samo nadawanie uprawnień polega na stworzeniu formularza, w którym wpisuje się od kiedy i do kiedy pracownik zostaje uprawniony do przetwarzania konkretnych danych osobowych. Warto też wskazać analogiczne informacje na temat dostępu do systemów informatycznych. Dobrą praktyką jest także wpisanie do takiego druku identyfikatora, jaki otrzymuje pracownik do posługiwania się tymi systemami. Jednocześnie w bibliotece powinna znajdować się ewidencja upoważnień, która stanowi kluczowy dokument z punktu widzenia wspomnianej wcześniej rozliczalności danych osobowych.

Ponadto, jednym z najważniejszych środków organizacyjnych zabezpieczenia danych osobowych jest wyznaczenie IOD. Oznacza to, że podstawowy środek organizacyjny wynika z obowiązku prawnego usankcjonowanego w art. 37 RODO. Wieloaspektowe zagadnienie wyznaczania IOD zostało szczegółowo omówione w rozdziale VII niniejszego Kodeksu. W zakresie środków organizacyjnych warto jednak podkreślić, że pozycja IOD w bibliotece będzie miała istotne znaczenie dla bezpieczeństwa danych osobowych i realnej kontroli nad poszczególnymi działaniami pod kątem ich ochrony. Predyspozycje IOD w zakresie wiedzy merytorycznej, ale też kompetencji społecznych, jak również relacje IOD z kadrą kierowniczą i pracownikami stanowią jeden z priorytetowych środków organizacyjnych zabezpieczenia danych. Rolą IOD jest też zapewnienie odpowiedniego przeszkolenia pracowników biblioteki osobiście lub poprzez wskazanie dyrekcji zapotrzebowania na organizację szkolenia zewnętrznego.

Pomimo tego, że środki organizacyjne zabezpieczenia danych osobowych należy traktować autonomicznie i obejmują one inne działania niż środki techniczne, zagadnienia te są ze sobą ściśle powiązane. Wynika to z przepisów RODO, których konstrukcja zakłada najczęściej, iż od ADO wymaga się zapewnienia kumulatywnie środków technicznych i organizacyjnych. Stąd też kluczowe jest, żeby zapewnić odpowiednie zastosowanie jednych i drugich, biorąc pod uwagę, że to od działań pracowników będzie zależała skuteczność większości środków technicznych. Jednocześnie odpowiedni dobór i wdrażanie środków technicznych będzie wynikało z właściwej organizacji pracy w bibliotece i zaangażowania wszystkich pracowników.

11 KONTROLA WEWNĘTRZNA I ZEWNĘTRZNA

11.1. Wewnętrzne sprawdzenie zgodności przetwarzania danych z przepisami.

Przepisy RODO są innowacyjne w stosunku do uprzednich przepisów o ochronie danych osobowych, gdyż wymagają od administratora danych dobierania technicznych i organizacyjnych środków ochrony danych do odpowiednich ryzyk i zagrożeń dla nich. Jednocześnie administrator danych ma obowiązek wynikający z art. 25 RODO stosowania zasady uwzględniania ochrony danych w fazie projektowania (privacy by desigin) oraz domyślnej ochrony danych (privacy by default). Zapewnienie monitorowania skuteczności tych zasad, czyli przetwarzania danych zgodnie z zasadami określonymi w art. 5 RODO jest bardzo istotnym elementem systemu ochrony danych osobowych. W bibliotece za monitorowanie zgodności przetwarzania danych z przepisami odpowiada inspektor ochrony danych. Obowiązujące przepisy o ochronie danych osobowych nie narzucają sztywnych kryteriów sposobu przeprowadzania sprawdzeń, ani ich częstotliwości, jednakże można wskazać dwa rodzaje wewnętrznych sprawdzeń: doraźne i planowane.

I. Sprawdzenia doraźne.

Sprawdzenia doraźne to szczególny rodzaj audytu, który jest wykonywany przez inspektora niezwłocznie, po stwierdzeniu naruszenia ochrony danych. Ma ono na celu ocenę ryzyka naruszenia praw i wolności osób, których dane dotyczą, ustalenia przyczyna wystąpienia zdarzenia, a także działań mających na celu ograniczenie skutków, w tym zapobiegających powtórzeniu się naruszenia w przyszłości.

Elementy sprawdzenia doraźnego:

- uzyskanie wyjaśnień od osób, które były zaangażowane w zdarzenie/miały wiedzę o zdarzeniu,
- ustalenie stanu faktycznego w oparciu o oględziny, wywiady, wgląd w obszary, których dotyczyło naruszenie,
- przygotowanie i przekazanie administratorowi zaleceń postępowania.

Wszystkie czynności powinny być wykonywane niezwłocznie – jeżeli naruszenie będzie wymagało zgłoszenia do Prezesa UODO, czas będzie miał ogromne zdarzenie. Inspektor nie musi wszystkich informacji uzyskiwać samodzielnie i bezpośrednio. Może zlecić bezpośrednim przełożonym zaangażowanych osób lub tym osobom, niezwłoczne przekazanie mu, np. w formie wiadomości e-mail,

niezbędnych wyjaśnień. Jego praca będzie polegała na analizie uzyskanych informacji, w tym ich konfrontacji, aby ustalić stan faktyczny. Każde sprawozdanie powinno kończyć sprawozdanie z naruszenia, które zostanie przekazane i omówione z dyrektorem biblioteki (Przykładowy wzór sprawozdania z naruszenia został podany w rozdziale 11.7. Dobre praktyki, wytyczne i wskazówki).

Sprawdzenie doraźne może być także wykonywane na prośbę administratora lub pracowników w związku z planowanym nowym procesem przetwarzania danych osobowych (np. konkurs, impreza, wysyłanie newslettera), jako element procesu prviacy by design, w tym jeżeli niezbędna jest ocena skutków dla ochrony danych.

II. Sprawdzenia planowane.

Okresowe, zaplanowane sprawdzenia to istotny aspekt pracy IOD, a także jeden z obowiązków ciążących na dyrektorze biblioteki w związku z ochroną danych osobowych. Monitorowanie zgodności przetwarzania danych powinno być ciągłym procesem, realizowanym na bieżąco przez inspektora. Im większa biblioteka i im więcej procesów przetwarzania danych, tym trudniejsze jest przeprowadzenie pełnego audytu. Dobrą praktyką jest monitorowanie mniejszych obszarów, w szczególności przeprowadzanie sprawdzeń w oparciu o procesy przetwarzania danych osobowych. Takie podejście pozwoli prześledzić zgodność przetwarzania danych osobowych na każdym etapie procesu, od zbierania danych, przez przesyłanie, przekazywanie, przechowywanie, modyfikowanie, udostępnianie, aż do archiwizacji lub zniszczenia. Dodatkowo należy uznać, że przeprowadzanie sprawdzeń dla konkretnych obszarów, a nie wszystkich procesów przetwarzania, pozwoli sprawdzenie przeprowadzić szybciej, dokładniej oraz na bieżąco przekazywać administratorowi zalecenia.

Przepisy RODO nie regulują częstotliwości oraz zakresu przeprowadzanych audytów, pozostawiając to w gestii inspektora wyznaczonego w bibliotece. Skuteczne działanie wymaga uzyskania wsparcia ze strony dyrektora biblioteki, więc każde planowane sprawdzenie powinno być wcześniej uzgodnione z dyrektorem, który przekaże pracownikom niezbędne polecenia służbowe w zakresie udzielania inspektorowi niezbędnych wyjaśnień oraz wspierania go podczas audytu. Każde sprawdzenie jest przeprowadzane dla administratora danych i powinien on być w nie zaangażowany i wspierać inspektora.

Czynności audytowe mają na celu sprawdzenie stanu faktycznego dotyczącego sposobu przetwarzania danych osobowych w ramach procesu przetwarzania, poprzez uzyskiwanie niezbędnych wyjaśnień, testowanie procesu (np. jeżeli dane są przetwarzane elektronicznie, analiza wprowadzania, przesyłu, przechowywania danych), uzyskanie wyjaśnień od osób, które przetwarzają dane w ramach procesu, sprawdzenie kto i w jakim zakresie ma dostęp do danych, analizę zabezpieczeń.

Elementy sprawdzenia:

- analiza legalności przetwarzanych danych,
- analiza adekwatności przetwarzanych danych do celu przetwarzania,
- ustalenie osób posiadających dostęp do danych w ramach procesu wraz z weryfikacją upoważnień i uprawnień,
- ustalenie czy wszystkie osoby posiadające dostęp do danych zostały zobligowane do zachowania poufności,
- realizacja obowiązków informacyjnych wobec osób, których dane dotyczą,
- realizacja pozostałych praw osób, których dane dotyczą,
- analiza zabezpieczeń technicznych,
- analiza zabezpieczeń teleinformatycznych,

- analiza zabezpieczeń organizacyjnych,
- analiza przepływu danych, w tym podmiotów, którym dane są udostępniane,
- analiza ryzyk związanych z procesem przetwarzania,
- ustalenie podmiotów przetwarzających dane w ramach procesu oraz analiza umów powierzenia,
- zalecenia dla administratora danych.

III. Sprawozdanie ze sprawdzenia.

Każde sprawdzenie powinno kończyć się sprawozdaniem ze sprawdzenia, które IOD omawia z administratorem. Dyrektor biblioteki może podjąć decyzję o niezastosowaniu zaleceń lub częściowym wdrożeniu zaleceń, jednakże powinien być świadomy z jakimi ryzykami wiąże się dany proces przetwarzania. Dobrą praktyką jest przekazywanie dyrektorowi biblioteki sprawozdania ze sprawdzenia nie tylko, aby przyjął je do wiadomości, ale także w celu podjęcia decyzji o sposobie postępowania. Decyzja administratora może zostać przez niego odnotowana w treści sprawozdania. Realizacja deklaracji administratora będzie podlegała analizie przy kolejnym sprawdzeniu. Jednym z często popełnianych błędów jest nie omawianie przez IOD wyników sprawdzenia z administratorem, podczas gdy wszystkie podejmowane przez inspektora czynności mają na celu wsparcie ADO w jego działaniach i powinien on brać aktywny udział w zapewnianiu ochrony danych osobowych w bibliotece. Miejsce przechowywania sprawozdań zależy od wewnętrznych ustaleń administratora. Jeżeli oryginały przechowuje dyrektor, wskazane jest aby kopie były u inspektora, gdyż są niezbędne do realizacji jego obowiązków oraz wykazania, że prawidłowo wywiązuje się ze swoich zadań.

11.2. Kontrole prowadzone przez Prezesa UODO.

Zasadniczo są trzy rodzaje postępowań, na które musi być przygotowany dyrektor biblioteki:

- „postępowanie doraźne", przeprowadzane w związku ze złożoną przez osobę, której dane dotyczą skargą, przeprowadzana drogą korespondencyjną;
- „postępowanie doraźne", przeprowadzane w związku ze złożoną przez osobę, której dane dotyczą skargą, przeprowadzana w siedzibie biblioteki;
- „postępowanie planowane", realizowane zgodnie z planem kontroli urzędu, zapowiadana około 2 tygodnie przed terminem przeprowadzenia.

Większość swoich działań nadzorczych Prezes UODO realizuje drogą korespondencyjną, gdy administrator danych jest wzywany do złożenia pisemnych wyjaśnień. Otrzymanie wezwania od urzędu nie oznacza, że administrator źle przetwarza dane osobowe, nie jest też wzywany do podejmowania natychmiastowych działań. Prezes UODO, gdy otrzymuje skargę na sposób przetwarzania danych przez administratora, ustala stan faktyczny, żądając od administratora niezbędnych informacji. Analiza wydanych przez urząd decyzji administracyjnych wskazuje, że w większości przypadków urząd odrzuca skargę lub uznaje postępowanie za bezprzedmiotowe, bo administrator po otrzymaniu listu z prośbą o złożenie wyjaśnień, dokonał analizy procesu przetwarzania i doprowadził do stanu zgodnego z przepisami prawa. Jeżeli Prezes UODO po uzyskaniu wyjaśnień od administratora, dochodzi do wniosku, że przetwarzanie przez niego danych narusza przepisy RODO, może nakazać administratorowi podjęcie konkretnych działań. W przypadku nie wykonania nakazu urzędu, administrator może oczekiwać powiadomienia o wszczęciu przez urząd postępowania kontrolnego. Prezes UODO może także podjąć decyzję o nałożeniu kary na administratora.

W przypadku przeprowadzania czynności kontrolnych w siedzibie administratora, inspektorzy UODO mają prawo wstępu do wszystkich pomieszczeń i przebywanie w siedzibie w godzinach 6-22. Dyrektor biblioteki nie może odmówić wpuszczenia inspektorów do siedziby biblioteki. W takim wypadku Prezes UODO jest uprawniony do uzyskania wsparcia funkcjonariuszy policji, aby uzyskać dostęp do budynku i pomieszczeń biblioteki, które mają podlegać kontroli. Obowiązkiem dyrektora jest wylegitymowanie inspektorów, w tym sprawdzenie ich tożsamości z dowodem osobistym oraz powiadomienie wszystkich pracowników o przeprowadzanej kontroli.

I. Udział IOD w kontroli.

Zgodnie z art. 38 RODO inspektor ochrony danych powinien być włączany we wszystkie sprawy związane z ochroną danych, w tym w czynności kontrolne prowadzone u administratora. Uczestnicząc w procesie kontroli będzie on w stanie wesprzeć ADO, a także udzielić inspektorom UODO niezbędnych wyjaśnień. Jako osoba odpowiedzialna za monitorowanie zgodności przetwarzania danych z przepisami, jest on najlepiej zorientowany we wszystkich procesach przetwarzania, w tym kto za nie odpowiada i od kogo można uzyskać wyjaśnienia. Inspektor jest łącznikiem pomiędzy administratorem i jego pracownikami, a inspektorami UODO i to on przekazuje im wszystkie niezbędne informacje.

II. Przebieg kontroli.

Czas i przebieg kontroli zależą w dużym stopniu od zakresu postępowania. Jeżeli Prezes UODO zapowiedział z wyprzedzeniem kontrolę, administrator i inspektor mieli czas na przygotowanie niezbędnych informacji. Inspektorzy UODO powinni mieć możliwość odnotowywania na bieżąco wyników kontroli, a także omawiania jej przebiegu, wskazane jest więc udostępnienie im niezbędnej przestrzeni biurowej. Informacje i wyjaśnienia powinny być precyzyjne i dotyczyć zadanego pytania. Inspektorzy realizują kontrolę w podobny sposób jak IOD przeprowadza sprawdzenie: analizują cały proces przetwarzania danych, sprawdzają i testują skuteczność zastosowanych środków zapewniających poufność, w tym zgodność z zasadami przetwarzania z art. 5 RODO. Szczególną uwagę inspektorzy przywiązują do realizacji praw osób, których dane dotyczą, w tym obowiązku informacyjnego.

Jeżeli kontrola wykaże, że administrator dokonuje przetwarzania w niewłaściwy sposób, wskazane jest, aby od razu zadeklarował jakie działania i w jakim czasie podejmie, a jeżeli to możliwe, nawet je podjąć.

III. Decyzja Prezesa UODO.

Po przeprowadzonej kontroli dyrektor biblioteki może oczekiwać decyzji Prezesa UODO, podsumowującej wyniki kontroli oraz w zależności od stwierdzonego stanu faktycznego nakazu i/lub zaleceń podjęcia odpowiednich działań. Prezes UODO może nakazać realizację tych działań w określonym czasie (np. 3 tygodni). Niewykonanie nakazu może skutkować nałożeniem pieniężnej kary administracyjnej na bibliotekę. Maksymalna kara, jaką może urząd nałożyć na bibliotekę wynosi 10 tys. złotych (art. 102 ustawy ODO). Jeżeli Prezes UODO uzna, że przemawia za tym interes publiczny, po zakończeniu postępowania informuje o wydaniu decyzji na stronie internetowej. Biblioteka wobec której została wydana prawomocna decyzja stwierdzająca naruszenie jest zobligowania podać

do publicznej wiadomości na swojej internetowej lub w BIP, informację o działaniach podjętych w celu wykonania decyzji (art. 73 ustawy UODO). Oznacza to, że zapewnienie właściwej ochrony danych osobowych jest też kwestią wizerunku biblioteki.

11.3. Kontrole prowadzone przez inne podmioty.

W przypadku audytów zewnętrznych, przeprowadzanych przez instytucje do tego wyznaczone takie jak: państwowe organy nadzoru i kontroli gospodarki finansowej, organy kontrolujące legalność, gospodarność, rzetelność organów administracji rządowej i organów samorządu terytorialnego, bądź stanowiące nadzór nad przestrzeganiem prawa pracy, konieczność i legalność ich wykonania wynika bezpośrednio z przepisów prawa powszechnie obowiązującego. Instytucje te działają między innymi w oparciu o ustawę zasadniczą, jaką stanowi Konstytucja RP oraz o inne przepisy rangi ustawowej np. ustawa o regionalnych izbach obrachunkowych, ustawa o NIK, ustawa o PIP, ustawa o samorządzie gminnym, ustawa o finansach publicznych, ustawa o samorządzie powiatowym. Przepisy prawne jednoznacznie wskazują zakres uprawnień organów przeprowadzających kontrole i określają zasady ich przeprowadzania.

I. Upoważnienie do przetwarzania danych osobowych dla kontrolującego.

Przetwarzanie danych osobowych na potrzeby kontroli przeprowadzanych przez uprawnione organy państwowe, regionalne, samorządowe w ramach działalności kontrolno-nadzorczej, która wiąże się z realizacją ustawowych obowiązków prawnych, jest legalne i nie wymaga upoważnienia do przetwarzania danych osobowych dla funkcjonariusza przeprowadzającego kontrole. W myśl art. 29 RODO podmiotem dopuszczonym do przetwarzania danych jest oprócz ADO także osoba przez niego upoważniona, działająca z jego polecenia. Upoważnienie udzielane przez ADO, określa jego zakres i okres obowiązywania. Należy podkreślić, że upoważnienie wystawione przez organ kontrolujący dla inspektorów przeprowadzających kontrole zewnętrzne, odnosi się wyłącznie do prawnego uzasadnienia prowadzonej kontroli, z którym związane jest między innymi przetwarzanie danych osobowych, do jej prawidłowego przeprowadzenia. Ważne jest, aby w upoważnieniu zostały właściwe określone podstawy prawne uprawniające do legalnego wglądu przez inspektora do dokumentacji podmiotu kontrolowanego. Przykładowo, nie ma prawnego uzasadnienia przeglądanie listy wynagrodzeń pracowników bez ich uprzedniej zgody przez przeprowadzającego kontrolę z ramienia jednostki samorządowej, który nie jest osobą upoważnioną ustawowo do kontrolowania placówki z przepisów prawa pracy. Niezależnie od tego, czy np. prezydent miasta stanowi nadzór nad instytucją, wgląd do danych w zakresie wynagrodzeń konkretnych pracowników jest niedozwolony – chyba, że kontrolujący wykaże podstawę prawną, która będzie go zwalniała z obowiązku uzyskania zgody. Wysokość wynagrodzenia za pracę jest daną chroniną i jej ujawnienie bez zgody pracownika, stanowi naruszenie w zakresie przetwarzania danych osobowych. Organem kontroli i nadzoru nad przestrzeganiem prawa pracy, w tym również w zakresie wynagrodzeń, jest Państwowa Inspekcja Pracy i społeczna inspekcja pracy działająca na szczeblu zakładowym i mimo, że urząd czy starostwo stanowią nadzór nad biblioteką nie posiadają kompetencji kontrolno-nadzorczych w zakresie prawa pracy.

II. Dokumenty okazywane przez przeprowadzającego kontrolę przed przystąpieniem do czynności kontrolnych.

Przeprowadzający kontrolę przed przystąpieniem do czynności kontrolnych, powinien okazać pisemne upoważnienie od organu zlecającego kontrolę, ze wskazaniem podstawy prawnej do przeprowadzenia kontroli oraz legitymację służbową. Są to dokumenty niezbędne do przeprowadzenia kontroli i powinny zostać okazane dyrektorowi biblioteki przed przystąpieniem do czynności kontrolnych. Upoważnienie do przeprowadzania kontroli powinno zawierać następujące dane:

- wskazanie organu kontrolującego,
- wskazanie podmiotu objętego kontrolą,
- określenie podstawy prawnej i zakresu przedmiotowego kontroli,
- imię i nazwisko, stanowisko służbowe osoby upoważnionej do przeprowadzenia kontroli,
- określenie daty rozpoczęcia i przewidywanego terminu zakończenia kontroli,
- podpis osoby udzielającej upoważnienia, z podaniem zajmowanego stanowiska lub funkcji,
- pouczenie kontrolowanego podmiotu o jego prawach i obowiązkach,
- datę i miejsce wystawienia upoważnienia.

Przeprowadzający kontrolę ma prawo wglądu do wszystkich niezbędnych do przeprowadzenia kontroli dokumentów, w tym dokumentów zawierających dane osobowe, a także poruszania się po placówce bez konieczności uzyskania dodatkowej przepustki, zgodnie z zakresem kontroli. Kontrolujący ma również prawo przeprowadzić postępowanie kontrolne lub poszczególne jego czynności w siedzibie organu kontrolującego. Dotyczy to np. analizy zebranych materiałów oraz notatek wykonanych podczas kontroli, pisania protokołu, czy wzywania pracowników do złożenia wyjaśnień w ramach kontroli.

III. Zakres uprawnień kontrolującego.

W zależności od organu kontrolującego przeprowadzający kontrolę, zgodnie z obowiązującymi ten organ przepisami ma prawo do:

- żądania niezbędnych informacji dotyczących działalności kontrolowanych jednostek,
- wstępu na teren i do pomieszczeń jednostek kontrolowanych,
- wglądu w dokumentację będącą przedmiotem kontroli,
- zabezpieczania dokumentów i innych dowodów,
- sporządzania lub zlecania sporządzenia niezbędnych do kontroli odpisów oraz wyciągów z dokumentów,
- przeprowadzania oględzin obiektów, maszyn i urządzeń oraz pomieszczeń,
- wzywania i przesłuchiwania osób w związku z kontrolą,
- wglądu do akt osobowych i wszelkich dokumentów związanych z wykonywaniem pracy przez pracowników lub osoby zatrudnione na innej podstawie niż stosunek pracy;
- zapoznania się z decyzjami wydanymi przez inne organy kontroli i nadzoru,
- utrwalenia przebiegu kontroli za pomocą środków technicznych służących do utrwalania obrazu lub dźwięku;
- wykonywania niezbędnych dla celów kontroli odpisów, zestawień lub wyciągów z dokumentów oraz obliczeń i zestawień sporządzanych na podstawie tych dokumentów,
- sprawdzania tożsamości osób wykonujących pracę lub przebywających na terenie podmiotu kontrolowanego.

Zakres uprawnień musi wynikać z przepisów prawa i nie może wykraczać poza ramy ustawowe obligujące inspektora reprezentującego organ przeprowadzający kontrolę do przeprowadzenia czynności kontrolnych.

11.4. Naruszenia ochrony danych osobowych i ich zgłaszanie do Prezesa UODO.

Zgłaszanie naruszeń ochrony danych do Prezesa UODO jest kolejną z innowacji wynikających z przepisów RODO. Administrator jest zobligowany poinformować organ nadzorczy o każdym naruszeniu, chyba że jest mało prawdopodobne, że naruszenie będzie skutkowało naruszeniem praw i wolności osób fizycznych (art. 33 RODO). Oceny ryzyka naruszenia w bibliotece dokonuje wyznaczony IOD w ramach przeprowadzanego sprawozdania doraźnego z naruszenia. Inspektor przekazuje ADO wyniki swojej analizy oraz rekomendacje. Należy podkreślić, że zgłoszenie naruszenia do organu jest czynnością techniczną i nie oznacza, że w jego wyniku organ nałoży na administratora pieniężną karę administracyjną. Celem dokonywania zgłoszeń jest uzyskiwanie przez organ niezbędnej wiedzy statystycznej o skali i rodzaju zagrożeń dla ochrony danych, a także umożliwienie organowi wspierania administratora w podjęciu niezbędnych działań, np. poprzez wydanie zaleceń w zakresie postępowania w celu ograniczenia skutków naruszenia. IOD jest punktem kontaktowym, do którego może zwrócić się urząd w celu uzyskania dodatkowych wyjaśnień.

I. Ocena ryzyka naruszenia dla praw i wolności osób fizycznych.

Naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Ryzyko naruszenia praw lub wolności oznacza skutek przetwarzania danych, mogący prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, w szczególności:

- jeżeli przetwarzanie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną,
- jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi,
- jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych,
- jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa,
- jeżeli oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych,

- jeżeli przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci,
- jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.

Jeżeli prawdopodobna jest materializacja przynajmniej jednego ze wskazanych ryzyk, dyrektor biblioteki ma obowiązek niezwłocznie, w czasie nieprzekraczającym 72 godziny, zawiadomić o naruszeniu Prezesa UODO. Niezależnie od zawiadomienia, dyrektor wraz IOD powinien podjąć działania mające na celu zminimalizowanie skutków naruszenia, np. ograniczyć dostępność danych, dokonać zmian ustawień systemowych, zmienić hasła do systemów informatycznych, przeszkolić personel). W szczególności dyrektor biblioteki może niezwłocznie wdrożyć zalecenia inspektora.

W każdej bibliotece powinna być sformalizowana oraz wdrożona procedura postępowania na wypadek wystąpienia naruszenia ochrony danych. Pozwoli to podjąć skuteczne działania we właściwym momencie, a także odpowiednio wcześniej zidentyfikować naruszenie. W szczególności można oprzeć tworzoną procedurę na Poradniku UODO „Obowiązki administratorów związane z naruszeniami ochrony danych osobowych"[24].

Procedura powinna zawierać co najmniej:

- określenie jakie zdarzenia należy uznać za naruszenie,
- zasady postępowania osoby, która stwierdziła naruszenie,
- obowiązki poszczególnych osób w związku z zaistniałym naruszeniem,
- metodę oceny ryzyka naruszenia praw i wolności osób, których dotyczy naruszenie,
- procedurę zawiadomienia Prezesa UODO o naruszeniu,
- procedurę zawiadomienia osób, których dotyczyło naruszenie.

Zgodnie z motywem 76 RODO oceniając ryzyko naruszenia praw i wolności osób fizycznych należy uwzględnić powagę zdarzenia (wielkości szkody, jakie zdarzenie to może spowodować w odniesieniu do osoby, której dane dotyczą) oraz (prawdopodobieństwa wystąpienia zdarzenia będącego skutkiem naruszenia). Oznacza to na konieczność udzielenia odpowiedzi na pytanie czy naruszenie może skutkować:

- Powstaniem uszczerbku fizycznego?
- Szkód majątkowych lub niemajątkowych u osób fizycznych, takich jak:
  - Utrata kontroli nad własnymi danymi osobowymi?
  - Ograniczenie praw?
  - Dyskryminacja?
  - Kradzież?
  - Sfałszowanie tożsamości?
  - Strata finansowa?
  - Nieuprawnione odwrócenie pseudonimizacji?
  - Naruszenie dobrego imienia?
  - Naruszenie poufności danych osobowych chronionych tajemnicą zawodową?
- Czy możliwe są inne znaczne szkody gospodarcze lub społeczne w wyniku naruszenia?

Zgodnie z art. 33 UODO zgłoszeniu nie podlegają naruszenia, dla których materializacja wskazanych negatywnych skutków dla osoby, której dane dotyczą jest mało prawdopodobna.

[24] Strona internetowa Urzędu Ochrony Danych Osobowych, https://uodo.gov.pl/pl/134/1029, [dostęp 08.10.2019].

II. Zawiadomienie Prezesa UODO o naruszeniu.

Administrator danych dokonuje zgłoszenia na formularzu udostępnionym na stronie organu, w formie elektronicznej (poprzez ePUAP lub podpis kwalifikowany) lub na piśmie (wysyłając list polecony). Każde zgłoszenie musi zawierać informacje wymagane art. 33 ust. 3 RODO:

- opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
- zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
- opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
- opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych.

Zgłoszenia dokonuje dyrektor biblioteki przy wsparciu inspektora. Inspektor nie może dokonywać zgłoszeń w imieniu administratora, o ile nie jest formalnym pełnomocnikiem biblioteki. W przypadku nieobecności dyrektora w momencie wystąpienia naruszenia, zgłoszenia powinna dokonać osoba uprawniona do pełnienia obowiązków pod jego nieobecność. Udział inspektora w zgłoszeniu może w szczególności polegać na wsparciu ADO w poprawnym wypełnieniu formularza zgłoszenia. Należy w nim zwrócić szczególną uwagę na określenie zidentyfikowanego ryzyka naruszenia praw i wolności osób, których dotyczyło naruszenie, a jeżeli administrator dokonywał zawiadomienia, należy dołączyć jego treść. Wszystkie przekazywane do urzędu informacji powinny zostać wcześniej zanonimizowane.

Jeżeli w momencie zidentyfikowania naruszenia nie da się udzielić pełnych wyjaśnień lub naruszenie nadal trwa, wówczas administrator dokonuje zgłoszenia wstępnego (opcja dostępna w formularzu) i sukcesywnie przekazuje administratorowi niezbędne informacje, aż do momentu zakończenia naruszenia.

Zgodnie z art. 33 ust. 5 wszystkie naruszenia powinny być ewidencjonowane, także te które nie podlegały zgłoszeniu do Prezesa UODO. Ewidencja powinna zawierać opis dokładnych okoliczności zdarzenia, jego skutki oraz podjęte działania. Ewidencję może prowadzić wyznaczony w bibliotece IOD.

11.5. Zawiadamianie osób, których dane dotyczą o naruszeniu.

I. Określenie konieczności dokonania zawiadomienia.

Ogólne rozporządzenie o ochronie danych osobowych wymaga, aby administrator danych dokonywał analizy skutków naruszenia ochrony danych dla praw i wolności osób, których dotyczy.

Ryzyko naruszenia praw lub wolności oznacza skutek przetwarzania danych, mogący prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych w szczególności, jeżeli:

- przetwarzanie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną,
- osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi,

- przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych,
- przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa,
- oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych,
- przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci,
- przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.

Dyrektor biblioteki dokonuje oceny ryzyka dla praw i wolności osób, których dotyczy naruszenia. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu (art. 34 RODO). Dla oszacowania ryzyka nie ma znaczenia ilu osób dotyczy naruszenie. Zawiadomienia należy dokonać, nawet jeżeli dotyczy tylko jednej osoby.

Dyrektor biblioteki nie będzie zobowiązany do dokonywania zawiadomienia, jeżeli spełniony jest którykolwiek z warunków określonych w artykule 34 ustęp 3 RODO:

- zostały wdrożone odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,
- zastosowano następnie (tzn. po wystąpieniu naruszenia) środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
- zawiadomienie wymagałoby niewspółmiernie dużego wysiłku.

Pierwszy warunek dotyczy działań podjętych przed wystąpieniem naruszenia. Na przykład, jeżeli w bibliotece stosuje się szyfrowanie danych osobowych, jako standardową metodę zabezpieczenia danych, w przypadku naruszenia ich poufności w postaci kradzieży danych, nie będzie obowiązku zawiadamiania osób, których dane dotyczą.

Drugi warunek odnosi się do działań podjętych po naruszeniu. Na przykład zostało wykryte włamanie do sytemu, ale administrator systemu zdążył naprawić lukę bezpieczeństwa w systemie, zanim nastąpił wyciek danych.

Trzeci warunek zwalniający powinien być stosowany z rozwagą. Dyrektor biblioteki stwierdzając niewspółmierność ma obowiązek ją wykazać i udokumentować, mając na względzie, że organ nadzorczy może ocenić jego decyzję jako niewłaściwą. Przykładem niewspółmierności byłaby sytuacja, gdyby zostały ujawnione dane adresowe kilku tysięcy osób, a jedyną formą kontaktu byłoby wysłanie listu poleconego. Gdyby koszt wysłania listów przekraczał możliwości finansowe biblioteki, można stwierdzić niewspółmierność. W takiej sytuacji musi zostać wydany publiczny komunikat lub zastosowany podobny środek, za pomocą którego osoby, których dane dotyczą, zostaną poinformowane w równie skuteczny sposób.

W dokonaniu oceny ryzyka związanego z wystąpieniem naruszenia, konieczności dokonania zawiadomienia, a także sposobu dokonania zawiadomienia, dyrektora biblioteki powinien wspierać inspektor ochrony danych. Należy go niezwłocznie włączać we wszystkie sprawy związane z ochroną danych osobowych.

II. Sposób dokonania zawiadomienia.

Przepisy o ochronie danych osobowych nie określają formy, w jakiej administrator dokonuje zawiadomienia, jednakże powinna ona być skuteczna oraz udokumentowana, aby można było wykazać skuteczne wywiązanie się z obowiązku prawnego. Forma zawiadomienia powinna być adekwatna do ryzyka związanego z naruszeniem, osób, których dotyczy, a także dostępnych środków przekazu. Jeżeli uległy ujawnieniu dane osobowe umożliwiające kradzież tożsamości, w szczególności zaciągnięcie zobowiązań na konto osoby, której dotyczy naruszenie, należy skorzystać ze środka komunikacji umożliwiającego jak najszybsze powiadomienie. Jeżeli zawiadomienie dotyczy niewielkiej grupy osób lub osób starszych, można powiadomić je telefonicznie. Jeżeli naruszenie dotyczy większej grupy, można wysłać wiadomości SMS-y i/lub wiadomości e-mail. Powiadomienie listowne powinno być wykorzystywane wówczas, gdy nie ma innej drogi komunikacji, przede wszystkim ze względu na czas związany z dostarczeniem powiadomienia. Przekazanie osobie, której dane dotyczą niezwłocznej informacji o zdarzeniu jest kluczowe, dla możliwości podjęcia przez nią działań, które są niezbędne do zapewnienia ochrony jej własnych interesów, w szczególności zastrzeżenia dokumentów, czy zmiany danych uwierzytelniających do systemu.

Dodatkowo wydanie publicznego komunikatu na stronie internetowej biblioteki jest dobrą praktyką oraz szansą na dotarcie do informacji przez osoby, których nie udało się skutecznie zawiadomić. Może to być także źródło konkretnych informacji o zdarzeniu, a także dalszych działaniach podjętych w celu ograniczenia skutków zdarzenia.

III. Treść zawiadomienia.

Zawiadomienie musi zostać przekazane prostym oraz zwięzłym językiem, a także zawierać informacje:

- imię i nazwisko oraz dane kontaktowe inspektora ochrony danych,
- o możliwych konsekwencjach naruszenia ochrony danych osobowych,
- o środkach zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

W bibliotece powinna być wdrożona oraz opracowana procedura dokonywania oceny ryzyka naruszenia, a także zawiadamiania osób, których dane dotyczą. Przekazując informacje o naruszeniu, należy położyć szczególny nacisk na zalecenia działań, które mogą zostać podjęte przez osobę, której dotyczy naruszenie, aby minimalizować jego skutki.

Jeżeli w momencie zawiadomienia, nie zostały jeszcze ustalone wszystkie okoliczności oraz konsekwencje zdarzenia, można informacje przekazywać sukcesywnie, w szczególności poprzez wydawania komunikatów na stronie internetowej. Treść zawiadomienia dołącza się do zgłoszenia naruszenia ochrony danych osobowych przekazywanego do Prezesa UODO.

IV. Udzielanie wyjaśnień.

Osoby, których dane dotyczą muszą mieć możliwość uzyskania szczegółowych wyjaśnień dotyczących naruszenia ich danych. Punktem kontaktowym w bibliotece jest inspektor ochrony danych. Jeżeli naruszenie dotyczy dużej liczby osób, dyrektor biblioteki może podjąć decyzję o zaangażowaniu dodatkowych osób, które wspomogą inspektora w udzielaniu wyjaśnień, a także uruchomić specjalny numer telefonu lub adres e-mail do wysyłania zapytań w sprawie naruszenia. Ze względu na możliwe

konsekwencje dla praw i wolności osób, których dane dotyczą, wszystkie wyjaśnienia powinny być udzielanie niezwłocznie, a odpowiedzi na najczęściej zadawane pytania mogą zostać zamieszczone na stronie internetowej biblioteki, aby przyśpieszyć udzielanie wyjaśnień.

11.6. Kary i odpowiedzialność administratora danych osobowych.

Skuteczność stosowania przepisów o ochronie danych osobowych jest w dużym stopniu zależna od obawy administratora przed potencjalną karą, której wysokość jest ustalana w odniesieniu do rocznych, światowych obrotów administratora. Kara pieniężna jest ustalana indywidualnie przez organ nadzorczy, w sposób proporcjonalny do czynu, w wysokości, która ma być odstraszająca. Jest ostatecznym środkiem, jaki stosuje organ nadzorczy.

Zgodnie z art. 58 ust. 2 RODO Prezes UODO w zakresie prowadzonych postępowań wobec administratora lub podmiotu przetwarzającego jest uprawniony do:

- wydawania ostrzeżeń dotyczących możliwości naruszenia przepisów RODO poprzez planowane operacje przetwarzania,
- udzielania upomnień w przypadku naruszenia przepisów RODO przez operacje przetwarzania,
- nakazania spełnienia żądania osoby, której dane dotyczą, wynikającego z praw przysługujących jej na mocy RODO,
- nakazania dostosowania operacji przetwarzania do przepisów RODO, a w stosownych przypadkach wskazanie sposobu i terminu,
- nakazania zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony jej danych,
- wprowadzania czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania,
- nakazania na mocy art. 16, 17 i 18 sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania oraz nakazanie na mocy art. 17 ust. 2 i art. 19 powiadomienia o tych czynnościach odbiorców, którym dane osobowe ujawniono,
- nakazania zawieszenia przepływu danych do odbiorcy w państwie trzecim lub do organizacji międzynarodowej.

Prezes UODO nakłada administracyjne kary pieniężne w zależności od okoliczności naruszenia, dodatkowo lub zamiast środków, o których mowa powyżej. Maksymalna administracyjna kara pieniężna, jaką może nałożyć Prezes UODO na bibliotekę została określona w art. 102 ust. 2 UODO i wynosi 10 tys. złotych. Podejmując decyzję o nałożeniu kary i ustalając jej wysokość organ nadzorczy dokonuje analizy okoliczności naruszenia jak:

- umyślny lub nie charakter, waga i czas trwania naruszenia,
- zakres danych, których dotyczy naruszenie,
- liczba poszkodowanych osób i rozmiar poniesionej przez nie szkody,
- postępowanie administratora przed i po stwierdzeniu naruszenia,
- stopień współpracy z organem podczas postępowania,
- wdrożone wcześniej środki techniczne i organizacyjne, w tym kodeksy postępowania lub certyfikacja,
- wcześniejsze naruszenia, które miały miejsce u administratora, a także sposób w jaki organ dowiedział się o naruszeniu; kategorie danych, których dotyczyło naruszenie,
- inne okoliczności, jak osiągnięcie na skutek naruszenia korzyści finansowej lub uniknięcie straty.

Powyższe elementy mają na celu jak najbardziej indywidualne podejście do każdego naruszenia, a także umożliwienie administratorowi wykazania podjęcia stosownych działań, które miały zminimalizować ryzyko naruszenia, a potem jego skutków. Okolicznością wpływającą bezpośrednio na możliwość nałożenia kary finansowej jest niezastosowanie przez bibliotekę środków nałożonych przez Prezesa UODO na mocy art. 58 ust. 2 RODO.

Skorzystanie przez Prezesa UODO ze środków dyscyplinujących przewidzianych w przepisach RODO nie wyłącza możliwości osoby, której dane dotyczą dochodzenia odszkodowania od administratora za naruszenie jej danych przed sądem.

Bardzo istotnym aspektem każdego naruszenia stwierdzonego u administratora jest utrata wizerunku, a także zaufania społecznego. Informacja o wycieku danych z biblioteki, która zostanie rozpowszechniona przez media, będzie miała bezpośredni wpływ na statystyki czytelnictwa w tej bibliotece, może także wpłynąć na globalne zmniejszenie zaufania społecznego wobec bibliotek. Czytelnik, aby skorzystać z biblioteki, podaje szeroki zakres swoich danych osobowych, który może zostać wykorzystany do kradzieży tożsamości lub zaciągnięcia pożyczki na jego dane. Dlatego zapewnienie bezpieczeństwa danych, to nie tylko obowiązek prawny dyrektora biblioteki, ale także dbałość o wysokie standardy obsługi użytkowników.


WYDAWNICTWO
NAUKOWE
I EDUKACYJNE
SBP