RODO w praktyce

– narzędzia do wykorzystania przy audycie systemu ochrony danych osobowych

Jakie narzędzia są niezbędne do przeprowadzenia audytu obecnego stanu zapewnienia ochrony danych osobowych w świetle przepisów o RODO? Jakie wzory są potrzebne przy stosowaniu nowych regulacji RODO? Wykorzystaj przykładowe wzory na bazie których opracujesz własne dokumenty.

DARIUSZ SKRZYŃSKI

Jednym z zadań w procedurze wdrażania RODO w bibliotece jest audyt obecnego systemu ochrony danych. Trzeba sprawdzić, w jaki sposób obecnie jednostka zapewnia ochronę danych osobowych pracowników, czytelników i innych osób, których dane osobowe przetwarza, aby ustalić, jak dużych modyfikacji należy dokonać. Aby jednak zrobić to porządnie, niezbędne są odpowiednia narzędzia, które to ułatwią. Oto przykładowe wzory, na bazie których można opracować własne dokumenty.

W nr. 2 znajdziesz wykaz zmian w ochronie danych osobowych, informacje o RODO oraz odpowiedzi na nurtujące pytania bibliotekarzy. Dodatkowo materiał zawiera przykładową procedurę przystosowania systemu ochrony danych do nowych regulacji.

KTO POWINIEN DOKONAĆ AUDYTU?

Analizę powinny przeprowadzić osoby odpowiedzialne w instytucji za projektowanie, wdrażanie, funkcjonowanie oraz ocenę skuteczności środków technicznych i organizacyjnych, których zadaniem jest zapewnienie odpowiedniego bezpieczeństwa danych osobowych. Po przeprowadzeniu analizy administrator bezpieczeństwa informacji (jeżeli funkcjonuje w bibliotece) lub dyrektor jako administrator powinien ocenić, czy bezpieczeństwo danych osobowych jest zapewnione na odpowiednim poziomie.

CO NALEŻY SPRAWDZIĆ?

Na tym etapie należy zapoznać się z RODO i artykuł po artykule ustalić, czy regulacja z przepisu jest wdrożona w bibliotece i w jakim stopniu. Wiem, że ta część wydaje się nie do przejścia, ale w taki sposób dyrektor (zespół osób powołanych do wdrożenia RODO) zapozna się z RODO jednocześnie sprawdzając, co należy poprawić we własnej organizacji, dokumentacji. Warto pamiętać, że ustawa – Przepisy wprowadzające ustawę o ochronie danych osobowych, która jest obecnie procedowana, może w stosunku do bibliotek publicznych ograniczyć stosowanie niektórych przepisów z RODO. Jednak nie warto czekać na nowe regulacje, bo może okazać się, że wtedy już nie będzie czasu, żeby wdrożyć RODO. Nawet jeżeli zaplanujemy wszystkie obowiązki z RODO, zawsze będzie można z nich zrezygnować lub zmodyfikować sposób postępowania.

Zamieszczam adres strony internetowej, na której można zapoznać się z projektem zmiany m.in. ustawy o bibliotekach i zweryfikować, które przepisy z RODO nie będą stosowane albo stosowane w ograniczonym zakresie: https://legislacja.rcl.gov.pl/projekt/12302951/katalog/12457712#12457712.

Poniżej (zob. wzór 1) zamieszczam zestawienie przepisów RODO, których stosowanie w bibliotece publicznej zostało częściowo ograniczone lub wyłączone, oraz listę kontrolną (zob. wzór 2).

Wzór 1. Wykaz przepisów RODO, których stosowanie zostało ograniczone

Przepis RODO	Zakres ograniczenia
Art. 5 ust. 2	Do ustawy o bibliotekach zostanie dodany m.in. nowy art. 6b, który wskazuje minimum danych osobowych, jakie przetwarzają biblioteki (imię, nazwisko, numer karty bibliotecznej, płeć, obywatelstwo, adres zamieszkania, itd.). Do przetwarzania tych danych osobowych nie stosuje się art. 5 ust. 2 RODO – w zakresie obowiązku wykazywania przestrzegania przepisów art. 5 ust. 1 RODO.
Art. 12	Podobnie jak powyżej do przetwarzania danych z art. 6b ograniczono stosowanie art. 12 i 15 RODO. Obowiązki z art. 12 RODO realizowane są bezpłatnie raz na sześć miesięcy. W pozostałych przypadkach administrator danych ma prawo pobrać opłatę w wysokości odpowiadającej kosztom sporządzenia odpowiedzi lub kopii danych.
Art. 15	
Art. 34	Przepisu art. 34 RODO nie stosuje się, jeśli administrator w terminie 72 godzin od stwierdzenia naruszenia ochrony danych osobowych wyda komunikat o naruszeniu na swojej stronie podmiotowej Biuletynu Informacji Publicznej lub na stronie internetowej.

Wzór 2. Lista kontrolna – zgodność systemu ochrony danych z RODO

RODO	Zagadnienie	Uwagi, wnioski	Stopień spełnienia
1.	2.	3.	4.
Zasady dotyczące przetwarzania danych i podstawy prawne przetwarzania			
Art. 5 ust. 1a	Przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość").		
Art. 5 ust. 1b	Zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ograniczenie celu").		
Art. 5 ust. 1c	Adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych").		
Art. 5 ust. 1d	Prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość").		
Art. 5 ust. 1d	Przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").		
Art. 5 ust. 1e	Przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania").		
Art. 5 ust. 2	Administrator jest odpowiedzialny za przestrzeganie przepisów dotyczących zasad przetwarzania danych i musi być w stanie wykazać ich przestrzeganie („rozliczalność").		

1.	2.	3.	4.
Art. 6	Przetwarzanie danych zwykłych posiada podstawę prawną.		
Art. 7 ust. 1	Jeżeli dane przetwarzane są na podstawie zgody, administrator jest w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie danych.		
Art. 7 ust 2	Jeżeli dane przetwarzane są na podstawie zgody, a zgoda jest wyrażana w pisemnym oświadczeniu, jest ona przedstawiona w sposób pozwalający wyraźnie odróżnić ją od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.		
Art. 7 ust. 3	Jeżeli dane przetwarzane są na podstawie zgody, wyrażona zgoda jest łatwa do wycofania.		
Art. 7 ust. 3	Jeżeli dane przetwarzane są na podstawie zgody, osoba, która zgodę ma wyrazić, jest informowana o prawie jej wycofania w każdej chwili przed jej wyrażeniem.		
Art. 7 ust. 4	Jeżeli dane przetwarzane są na podstawie zgody, od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.		
Art. 9	Przetwarzanie szczególnych kategorii danych osobowych posiada podstawę prawną.		
Warunki wyrażenia zgody przez dziecko w przypadku usług społeczeństwa informacyjnego			
Art. 8 ust. 1	Jeżeli dziecko nie ukończyło 16 lat, zgodę na przetwarzanie danych wyraziła lub zaaprobowała osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody (polski ustawodawca ma ten wiek ograniczyć do 13 lat).		
Art. 8 ust. 2	Administrator, uwzględniając dostępną technologię, podejmuje rozsądne starania, by zweryfikować, czy osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem wyraziła zgodę lub ją zaaprobowała.		
Przejrzystość i tryb korzystania z praw			
Art. 12 ust. 1	Informacje podawane w obowiązku informacyjnym oraz komunikacja w sprawach art. 15-22 RODO udzielane są w zwięzłej, przejrzystej, zrozumiałej formie i łatwo dostępnej formie.	Obowiązki z art. 12 realizowane są bezpłatnie raz na sześć miesięcy. W pozostałych przypadkach administrator danych ma prawo pobrać opłatę w wysokości odpowiadającej kosztom sporządzenia odpowiedzi lub kopii danych.	
Art. 12 ust. 2	Administrator ułatwia osobie, której dane dotyczą, uzyskanie wszelkich informacji w przedmiocie przetwarzanych danych.		
Art. 12 ust. 3	Administrator bez zbędnej zwłoki, a w każdym razie w terminie miesiąca od otrzymania żądania, udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem na podstawie art. 15-22.		
Art. 12 ust. 3	Jeżeli występuje przedłużenie terminu do spełnienia żądań osoby, której dane dotyczą, w ramach art. 15-22, występuje to z uwagi na skomplikowany charakter żądania lub liczbę żądań. Czas udzielenia informacji jest jednak nie dłuższy niż dalsze dwa miesiące.		
Art. 12 ust. 4	Jeżeli administrator nie podejmuje działań w związku z żądaniem osoby w ramach art. 15-22, której dane dotyczą, niezwłocznie, lecz nie później niż w terminie miesiąca od otrzymania żądania informuje o: powodach niepodjęcia działań; możliwości wniesienia skargi do organu nadzorczego; skorzystania z ochrony prawnej przed sądem.		
Art. 12 ust. 5	Obowiązek informacyjny oraz wykonywanie praw przysługujących osobie, której dane dotyczą, w ramach art. 15-22 odbywa się bez pobierania opłat.		

1.	2.	3.	4.
Art. 12 ust. 5	Odmówienie podjęcia działań w związku z żądaniem na podstawie art. 15-22 lub pobieranie rozsądnej opłaty następuje, jeżeli żądania osoby są nadmierne lub ewidentnie nieuzasadnione w szczególności ze względu na swój ustawiczny charakter.	Obowiązki z art. 12 realizowane są bezpłatnie raz na sześć miesięcy. W pozostałych przypadkach administrator danych ma prawo pobrać opłatę w wysokości odpowiadającej kosztom sporządzenia odpowiedzi lub kopii danych.	
Art. 12 ust. 5	Jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby składającej żądanie w zakresie art. 15-22, żąda dodatkowych informacji niezbędnych do potwierdzenia tożsamości.		
Weryfikacja dopełnienia obowiązku informacyjnego w przypadku gromadzenia danych od osoby, której dane dotyczą, oraz z innych źródeł			
Art. 13 i 14	Swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela.		
Art. 13 i 14	Gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych (tymczasowo ABI).		
Art. 13 i 14	Cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania.		
Art. 13 i 14	Jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią.		
Art. 13 i 14	Informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją.		
Art. 13 i 14	Gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.		
Art. 13 i 14	Okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu.		
Art. 13 i 14	Informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych.		
Art. 13 i 14	Jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.		
Art. 13 i 14	Informacje o prawie wniesienia skargi do Prezesa UODO.		
Art. 13 i 14	Informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych.		
Art. 13 i 14	Informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, 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.		
Art. 14	W przypadku zbierania danych nie od osoby, której one dotyczą, informację o źródle pochodzenia danych, a jeśli ma to zastosowanie, czy pochodzą one ze źródeł publicznie dostępnych.		

1.	2.	3.	4.
Art. 13 ust. 3 i 14 ust. 4	Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji.		
Art. 14 ust. 3	Informacje wynikające z obowiązku informacyjnego, w przypadku zbierania danych osobowych nie od osoby, której dotyczą, podawane są: 1. w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych; 2. jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.		
Prawa osób, których dane dotyczą			
Art. 15	Realizowanie prawa dostępu przysługującego osobie, której dane dotyczą. W tym wydawanie kopii danych.	Obowiązki z art. 15 realizowane są bezpłatnie raz na sześć miesięcy. W pozostałych przypadkach administrator danych ma prawo pobrać opłatę w wysokości odpowiadającej kosztom sporządzenia odpowiedzi lub kopii danych.	
Art. 16	Realizowanie prawa do sprostowania danych.		
Art. 17	Realizowanie prawa do usunięcia danych (prawo do bycia zapomnianym).		
Art. 18	Realizowanie prawa do ograniczenia przetwarzania.		
Art. 19	Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania.		
Art. 20	Realizowanie prawa do przenoszenia danych.		
Prawo do sprzeciwu			
Art. 21 ust. 1	Możliwość wniesienia sprzeciwu przez osobę, której dane dotyczą – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e (wykonanie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej) lub f (prawnie usprawiedliwiony cel administratora danych lub strony trzeciej), w tym profilowania na podstawie tych przepisów.		
Art. 21 ust. 4	Poinformowanie osoby, której dane dotyczą, najpóźniej przy okazji pierwszego kontaktu, w sposób jasny i odrębny od wszelkich innych informacji o możliwości wniesienia sprzeciwu.		
Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie			
Art. 22 ust. 1	Niepodejmowanie decyzji względem osoby, której dane dotyczą, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.		
Art. 22 ust. 3	Jeżeli profilowanie jest dopuszczalne, administrator danych wdraża właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji.		
Art. 22 ust. 3	Niepoddawanie profilowaniu danych szczególnej kategorii, chyba że osoba, której dane dotyczą, wyraziła zgodę lub przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, i istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.		

1.	2.	3.	4.
Obowiązki administratora danych			
Art. 24 ust. 1	Poddawanie przeglądom i uaktualnianie stosowanych technicznych i organizacyjnych środków ochrony danych osobowych.		
Art. 24 ust. 2	Wdrożenie przez administratora danych odpowiednich polityk ochrony.		
Art. 24 ust. 3	Stosowanie przez administratora danych zatwierdzonych kodeksów postępowania lub zatwierdzonego mechanizmu certyfikacji.		
Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych			
Art. 25 ust. 1	Uwzględnianie ochrony danych w fazie projektowania.		
Art. 25 ust. 2	Domyślna ochrona danych (np. pseudonimizacja).		
Art. 27 ust. 1	Wyznaczenie na piśmie przedstawiciela na terenie UE.		
Art. 28 ust. 1	Korzystanie przez administratora danych 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.		
Art. 28 ust. 2	Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora.		
Elementy umowy o powierzeniu przetwarzania			
Art. 28 ust. 3	Przedmiot i czas trwania przetwarzania.		
Art. 28 ust. 3	Charakter i cel przetwarzania.		
Art. 28 ust. 3	Rodzaj danych osobowych oraz kategorie osób, których dane dotyczą.		
Art. 28 ust. 3	Obowiązki i prawa administratora danych.		
Art. 28 ust. 3 lit. a	Wskazanie, że przetwarzanie danych odbywa się wyłącznie na udokumentowane polecenie administratora.		
Art. 28 ust. 3 lit. b	Zapewnienie, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy.		
Art. 28 ust. 3 lit. c	Podejmuje środki bezpieczeństwa danych (art. 32 RODO).		
Art. 28 ust. 3 lit. d	Zobowiązanie podmiotu przetwarzającego do przestrzegania warunków korzystania z usług innego podmiotu przetwarzającego.		
Art. 28 ust. 3 lit. e	Pomoc administratorowi danych poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą.		
Art. 28 ust. 3 lit. f	Pomoc administratorowi danych w wywiązaniu się z obowiązku zapewnienia bezpieczeństwa danych, zgłaszania naruszeń ochrony danych osobowych organowi nadzorczemu, zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, oceny skutków przetwarzania, uprzednich konsultacji (art. 32-36 RODO).		
Art. 28 ust. 3 lit. g	Zobowiązanie do usunięcia lub zwrotu administratorowi danych wszelkich danych osobowych oraz usunięcie wszelkich ich istniejących kopii, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.		
Art. 28 ust. 3 lit. h	Zobowiązanie do udostępnienia administratorowi danych wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w art. 28 RODO oraz umożliwienie administratorowi danych lub audytorowi upoważnionemu przez administratora danych przeprowadzanie audytów, w tym inspekcji, i przyczynianie się do nich.		

1.	2.	3.	4.
Przetwarzanie z upoważnienia administratora lub podmiotu przetwarzającego			
Art. 29	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.		
Rejestrowanie czynności przetwarzania			
Art. 30 ust. 1	Prowadzenie w formie pisemnej, w tym elektronicznej, rejestru czynności przetwarzania danych osobowych, za które odpowiadają.		
Współpraca z Prezesem UODO			
Art. 31	Administrator lub podmiot przetwarzający (ewentualnie przedstawiciel) współpracuje z organem nadzorczym w ramach wykonywania przez niego swoich zadań.		
Bezpieczeństwo danych osobowych			
Art. 32 ust. 1 i 2	Administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku, uwzględniając stan wiedzy technicznej, koszt wdrożenia oraz charakter, zakres, kontekst i cel przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia. Uwzględnienie w szczególności ryzyka wiążącego się z przetwarzaniem (szacowanie ryzyka), w szczególności wynikające z: – przypadkowego lub niezgodnego z prawem zniszczenia; – utraty, modyfikacji, nieuprawnionego ujawnienia; – nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.		
art. 32 ust. 1 a-d	Administrator i podmiot przetwarzający wdrożyli m.in.: – pseudonimizację i szyfrowanie danych osobowych, – zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, – zdolność do szybkiego przywracania 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.		
art. 32 ust. 3	Administrator i podmiot przetwarzający stosują zatwierdzony kodeks postępowania lub zatwierdzony mechanizm certyfikacji celem wykazania wdrożenia odpowiednich środków technicznych i organizacyjnych dla bezpieczeństwa danych osobowych.		
art. 32 ust. 4	Administrator oraz podmiot przetwarzający podjęli działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego.		
Zgłaszanie naruszenia ochrony danych osobowych Prezesowi UODO			
art. 33 ust. 1	Zgłaszanie naruszenia ochrony danych osobowych powodujące ryzyko naruszenia praw i wolności osób fizycznych przez administratora w terminie 72 godzin po stwierdzeniu naruszenia do organu nadzorczego.		
art. 33 ust. 2	Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.		
art. 33 ust 1 a-d	Zgłoszenie zawiera wymagane elementy.		
art. 33 ust. 5	Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.		

1.	2.	3.	4.
Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych			
art. 34 ust. 1	O naruszeniu ochrony danych osobowych powodującym wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.	Przepisu art. 34 RODO nie stosuje się, jeśli administrator w terminie 72 godzin od stwierdzenia naruszenia ochrony danych osobowych wyda komunikat o naruszeniu na swojej stronie podmiotowej Biuletynu Informacji Publicznej lub na swojej stronie internetowej.	
art. 34 ust. 2	Zawiadomienie jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b, c i d RODO.		
Ocena skutków dla ochrony danych i uprzednie konsultacje			
art. 35 ust. 1 i 3	Administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, gdy przetwarzanie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Wymagana w szczególności w przypadku: – systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną; – przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10; lub – systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.		
art. 35 ust. 2	Dokonując oceny skutków dla ochrony danych, administrator konsultuje się z inspektorem ochrony danych, jeżeli został on wyznaczony.		
art. 35 ust. 7	Ocena skutków przetwarzania zawiera co najmniej elementy wskazane w art. 35 ust. 7 RODO.		
art. 35 ust. 11	Gdy zmienia się ryzyko wynikające z operacji przetwarzania, administrator dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych		
Uprzednie konsultacje			
art. 36 ust. 1	Administrator konsultuje się z organem nadzorczym przed rozpoczęciem przetwarzania, jeżeli ocena skutków dla ochrony danych, wykazała, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka.		
art. 36 ust. 3	Konsultując się z organem nadzorczym, administrator przedstawił mu wymagane elementy określone w art. 36 ust. 3 RODO.		
Ocena skutków dla ochrony danych i uprzednie konsultacje			
art. 37 ust. 1 a-c	Wyznaczenie inspektora ochrony danych przez administratora lub podmiot przetwarzający w sytuacjach obligatoryjnych.		
art. 37 ust. 2 i 3	W przypadku wyznaczenia jednego inspektora ochrony danych: – czy łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej, – przez kilka organów lub podmiotów publicznych, został on wyznaczony z uwzględnieniem ich struktury i wielkości.		
art. 37 ust. 5	Inspektor ochrony danych został wyznaczony na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełniania zadań nałożonych przez RODO.		
art. 37 ust. 7	Administrator lub podmiot przetwarzający publikują dane kontaktowe inspektora ochrony danych i zawiadamiają o nich organ nadzorczy.		

1.	2.	3.	4.
Status inspektora ochrony danych			
art. 38 ust. 1	Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.		
art. 38 ust. 2	Administrator oraz podmiot przetwarzający wspierają inspektora ochrony danych w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.		
art. 38 ust. 3	Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.		
art. 38 ust. 4	Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia.		
art. 38 ust. 6	Inspektor ochrony danych może wykonywać inne zadania i obowiązki. Administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów.		
Ocena skutków dla ochrony danych i uprzednie konsultacje			
art. 39 ust. 1a	Inspektor informuje administratora, podmiot przetwarzający oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie.		
art. 39 ust. 1b	Inspektor monitoruje przestrzeganie niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty.		
art. 39 ust. 1c	Inspektor udziela na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowania jej wykonania zgodnie z art. 35 RODO.		
art. 39 ust. 1d	Inspektor współpracuje z Prezesem UODO.		
art. 39 ust. 1e	Inspektor pełni funkcje punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzi konsultacje we wszelkich innych sprawach.		
art. 39 ust. 2	Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.		
Przekazywanie danych osobowych do państwa trzeciego			
Art. 45 ust. 1 w zw. z ust. 3	Przekazywanie danych osobowych do państwa trzeciego znajduje podstawę w decyzji Komisji.		
Art. 46	Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej następuje poprzez zapewnienie odpowiednich zabezpieczeń, i pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej.		
Art. 46 ust. 5	Przekazywanie danych znajduje podstawę w decyzji wydanej przez GIODO, która dotychczas nie została zmieniona, zastąpiona, uchylona.		
Art. 49	Jednorazowe lub wielokrotne przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej następuje na podstawie jednego z wyjątków.		

.....

podpis ABI/IOD

AKTUALIZACJA OBECNEJ DOKUMENTACJI OCHRONY DANYCH

W kolejnym kroku należy dostosować dokumentację ochrony danych na podstawie stwierdzonych ustaleń. Po przeprowadzonej analizie większość obecnych polityk i instrukcji można dalej wykorzystać, pod warunkiem dostosowania ich do wymagań RODO. Nie sposób sobie wyobrazić, że biblioteka zlikwiduje instrukcje, politykę czy nadane upoważnienia tylko dlatego, że RODO wprost nie wymaga tych dokumentów. Proszę zauważyć, że w dalszym ciągu przepisy wymagają zapewnienia wymogów bezpieczeństwa, w tym wdrożenie odpowiednich środków technicznych i organizacyjnych, aby zapewnić stosowny stopień bezpieczeństwa. Zatem te dokumenty powinny nadal obowiązywać. Na dokumentację po 25 maja 2018 r. można wykorzystać dotychczasowe materiały:

- politykę bezpieczeństwa;
- instrukcję zarządzania systemami informatycznymi;
- ewidencje osób upoważnionych;
- zawarte umowy powierzenia;
- wzory upoważnień dla osób dopuszczonych do przetwarzania danych.

Oczywiście dokumentację należy przejrzeć, udoskonalić i dostosować do RODO.

Jeżeli jednak biblioteka nie miała rzetelnej dokumentacji (np. niepełną, niedostosowaną do działalności biblioteki), to niestety będzie miała większe problemy, bo od początku będzie musiała badać, gdzie i na jakiej podstawie są przetwarzane dane.

RODO wymaga m.in., by dodatkowo wprowadzić następujące dokumenty:

- rejestr czynności przetwarzania;
- ewidencja i zgłoszenie naruszenia ochrony danych;
- komunikat o zaistniałym naruszeniu do zamieszczenia na www lub BIP;
- nowe klauzule informacyjne.

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

Proponuję jednak zacząć nie od aktualizacji polityk czy instrukcji, ale od stworzenia rejestru czynności przetwarzania danych osobowych. Jeżeli w bibliotece jest polityka bezpieczeństwa przetwarzania danych osobowych, załącznikiem do niej powinien być wykaz zbiorów danych osobowych. Można wykorzystać ten dokument i na jego bazie uzupełnić pozostałe informacje, jakie powinny znaleźć się w rejestrze. Dane te zawiera art. 30 RODO. Jeżeli jakiś zbiór został pominięty, należy go odnotować. Dostosowując treść obecnego dokumentu można uniknąć konieczności tworzenia dodatkowych dokumentów. Można zmienić dotychczasowy załącznik i określić, że teraz ten wykaz będzie się nazywał rejestrem czynności przetwarzania danych (zob. wzór 3).

Co prawda z RODO wprost nie wynika, że biblioteka jest zobowiązana do prowadzenia tego rejestru (zob. art. 30 ust. 5 RODO), ale pozwoli to zorientować się, jakiego rodzaju dane, jakich podmiotów, w jakim celu, na jakiej podstawie prawnej są gromadzone. Ponadto nie można wykluczyć, że przetwarzanie danych może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, albo że przetwarzanie nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych (taka nazwa zastępuje określenie danych wrażliwych).

Wzór 3. Rejestr czynności przetwarzania danych osobowych

.....

nazwa administratora, dane kontaktowe

.....

imię i nazwisko IOD, dane kontaktowe

Kategorie osób, których dane dotyczą	Kategorie danych osobowych	Cel przetwarzania danych osobowych	Odbiorca lub kategoria odbiorców, którym mogą być przekazywane dane osobowe	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (art. 32 RODO) (jeżeli jest to możliwe)	Informacja dotycząca przekazywania danych do państwa trzeciego	Planowane terminy usunięcia danych (jeżeli jest to możliwe)
Np. Pracownicy	*Np. imię, nazwisko, nr PESEL, nr NIP, adres zamieszkania.*		*Np. Dane nie są ujawniane odbiorcom.*		*Np. Dane nie są przekazywane*	

Jeżeli w ramach któregoś ze zbiorów biblioteka stwierdzi, że podstawą przetwarzania jest zgoda, należy upewnić się, czy mamy taką zgodę użytkownika odnotowaną i czy jej treść odpowiada wymogom stawianym przez RODO (art. 13). W sytuacji, gdyby zgoda okazała się odebrana wadliwie, trzeba zaplanować procedurę uzyskania zgody jeszcze raz, tym razem już poprawnej i odpowiadającej wymogom RODO.

Najważniejsze zmiany jednak polegają przede wszystkim na potwierdzeniu w treści RODO warunków wyrażenia zgody (art. 7 RODO). Żeby przetwarzanie danych na podstawie zgody było legalne (np. na potrzeby konkursu), należy zapewnić:

- **możliwość wycofania zgody w łatwy sposób i w dowolnym momencie** – jeśli administrator planuje uzyskiwać zgodę, powinien już na tym wstępnym etapie przewidzieć mechanizm jej wycofania, a więc zastanowić się, jak zgodę tę będzie można odwołać (gdzie rodzic musi się zgłosić, jaki dokument wypełnić);
- **dobrowolność wyrażenia zgody** – chodzi o to, żeby nie uzależniać podjęcia pewnych działań od wyrażenia zgody (np. udziału w konkursie od wyrażenia zgody na przetwarzania zgody przez podmiot fundujący nagrodę w konkursie);
- **zapewnienia, aby osoba wyrażająca zgodę rozumiała istotę zgody, jej cel i skutki**, pełne rozeznanie, konkretnie przez kogo i w jakim celu jej dane będą przetwarzane;
- **możliwość udowodnienia uzyskania zgody** – jeśli administrator nie jest w stanie tego wykazać, nie dysponuje podstawą prawną umożliwiającą mu przetwarzanie danych osobowych.

Biblioteka nie musi pozyskiwać nowych zgód po 25 maja br. na wykorzystanie danych pod warunkiem, że zebrane zgody odpowiadają warunkom RODO (zob. wzór 4). Tak wskazano w motywie 171 preambuły RODO.

Przy okazji warto zapoznać się bliżej z zasadami wyrażania zgody przez uczniów w przypadku tzw. usług społeczeństwa informacyjnego – to jedna z nowości wprowadzona w RODO. Zgodnie z art. 8 ust. 1 RODO, jeżeli zastosowanie ma zgoda na przetwarzanie danych osobowych, zgodne z prawem jest przetwarzanie danych osobowych dziecka, które ukończyło 16 lat. Jeżeli natomiast dziecko nie ukończyło 16 lat (w Polsce ma być 13 lat), takie przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy zgodę wyraziła lub zaakceptowała ją osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem. Wydawałoby się, że przepisy o zgodach wyrażanych przez dzieci dotyczyć będą raczej podmiotów świadczących usługi elektroniczne. Jeżeli jednak dzieci korzystają z internetu i uczestniczą w projektach, gdzie zaczyna się przetwarzać dane osobowe w szerszym zakresie i trochę inaczej niż tylko w związku z realizacją prawa oświatowego, w takich przypadkach pojawia się problem pytania o zgodę oraz jej konstrukcji, bo mamy do czynienia ze świadczeniem usług społeczeństwa informacyjnego, o którym wspomina RODO.

Wzór 4. Lista kontrolna – jakie wymogi musi spełniać klauzula zgody na przetwarzanie danych osobowych zgodnie z RODO

Zadbaj o odpowiednią formę zebranej zgody	Tak/Nie
Zbierz zgodę w taki sposób, żebyś mógł udowodnić, że osoba, której dane przetwarzasz, wyraziła na to zgodę. Zalecana jest forma pisemna, ale możesz też mieć nagrania, na których podmiot danych wyraża zgodę, albo odpowiednio zapisane zgody w systemie informatycznym.	
Możesz połączyć klauzulę zgody z innym oświadczeniem, ale musi być ona wyraźna	
Jeżeli osoba, której dane dotyczą, wyraża zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. W przeciwnym wypadku taka zgoda będzie nieważna.	
Uwzględnij prawo do wycofania zgody	
Zapewnij osobie, której dane dotyczą, prawo do wycofania zgody w dowolnym momencie.	
Zanim osoba, której dane dotyczą, wyrazi zgodę, poinformuj ją o tym, że może wycofać zgodę.	
Zapewnij, aby wycofanie zgody było równie łatwe jak jej wyrażenie.	
Nie wymuszaj zgody	
Jeżeli przetwarzanie danych nie jest niezbędne do realizacji umowy, nie możesz uzależnić wykonania umowy od wyrażenia zgody na przetwarzanie danych osobowych.	
Zbieraj zgody jedynie od osób, które ukończyły co najmniej 16 lat	
Jeśli świadczysz usługi społeczeństwa informacyjnego oferowane bezpośrednio dziecku, możesz uzyskać zgodę na przetwarzanie danych osobowych tylko od dziecka, które ukończyło 16 lat (polski ustawodawca planuje obniżyć tę granicę do 13 lat). W przeciwnym wypadku zgodę udzielają osoby sprawujące nad nimi władzę rodzicielską lub opiekę.	
Uwzględniając dostępną technologię, podejmij rozsądne starania, by zweryfikować, czy osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem wyraziła zgodę lub ją zaaprobowała.	

UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Jeżeli przetwarzanie danych osobowych biblioteka powierza choćby podmiotowi udostępniającemu BIP, koniecznie jest przejrzenie tych dokumentów. RODO wymaga, by zasady ich współpracy z bibliotekami były precyzyjnie określone (może być nie tylko umowa pisemna, ale i elektroniczna). RODO wspomina o umowie lub innym instrumencie prawnym, który wskazuje: przedmiot, czas trwania przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, a także cel przetwarzania informacji (art. 28 RODO). Zatem nie jest to nowy standard, ale należy skontrolować zawarte z podwykonawcami umowy pod kątem wymagań nowych przepisów. Przepisy zakazują zewnętrznym firmom przekazywania informacji innym podmiotom bez uzyskania zgody administratora. Należy zabezpieczyć się stosownymi oświadczeniami w umowach powierzenia. Warto sprawdzić, czy podmioty, którym powierzamy dane, zapewniają stosowanie odpowiednich środków ochrony danych osobowych (zob. wzór 5).

Wzór 5. Lista kontrolna – jak powierzyć przetwarzanie danych osobowych zgodnie z RODO

Wybierz rzetelną firmę, której powierzysz przetwarzanie danych osobowych	Tak/Nie
Jeżeli powierzasz przetwarzanie danych osobowych innemu podmiotowi, wybierz taki, który zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, które będą spełniały wymogi ogólnego rozporządzenia o ochronie danych osobowych i chroniły prawa osób, których dane dotyczą.	
Zawrzyj z podmiotem przetwarzającym umowę powierzenia przetwarzania danych osobowych	
W umowie powierzenia przetwarzania danych osobowych wskaż przedmiot i czas trwania przetwarzania danych.	
W umowie powierzenia przetwarzania danych osobowych wskaż charakter i cel przetwarzania danych.	
W umowie powierzenia przetwarzania danych osobowych wskaż rodzaj powierzanych danych osobowych do przetwarzania.	
W umowie powierzenia przetwarzania danych osobowych wskaż swoje obowiązki i prawa.	
W umowie powierzenia przetwarzania danych osobowych wskaż kategorie osób, których dane dotyczą.	
Zapisz w umowie powierzenia przetwarzania danych osobowych obowiązek zachowania danych osobowych w tajemnicy	
Zobowiąż podmiot przetwarzający, by zapewnił, że osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy.	
Zobowiąż podmiot przetwarzający, by pomagał realizować prawa podmiotów danych	
W umowie powierzenia przetwarzania danych osobowych zobowiąż podmiot przetwarzający, żeby w miarę możliwości pomagał ci realizować prawa osób, których dane są przetwarzane.	
Zagwarantuj sobie prawo kontroli	
Zapisz w umowie powierzenia przetwarzania danych osobowych możliwość prowadzenia przez ciebie lub upoważnionego audytora możliwość przeprowadzania audytów, w tym inspekcji u podmiotu przetwarzającego powierzone dane.	
Zabezpiecz się na wypadek, gdy podmiot przetwarzający będzie chciał powierzyć przetwarzanie danych swojemu podwykonawcy	
Zapisz w umowie powierzenia przetwarzania danych osobowych, że w sytuacji, gdy podmiot przetwarzający będzie chciał podpowierzyć przetwarzanie danych osobowych swojemu wykonawcy, musi każdorazowo uzyskać twoją zgodę.	
Jeżeli udzielasz przetwarzającemu ogólnej zgody na korzystanie z podwykonawców przy przetwarzaniu powierzonych danych osobowych, zobowiąż go, żeby informował cię o każdym nowym podwykonawcy.	
Zagwarantuj sobie w umowie powierzenia przetwarzania danych osobowych, że możesz nie zgodzić się na zaproponowanego przez podmiot przetwarzający podwykonawcę.	
Określ w umowie powierzenia przetwarzania danych osobowych, że podwykonawca musi spełnić takie same warunki, jak podmiot przetwarzający w zakresie dbania o ochronę danych osobowych.	
Zobowiąż podmiot powierzający do usunięcia lub zwrotu danych po zakończeniu przetwarzania	
Zapisz w umowie powierzenia przetwarzania danych osobowych, że po zakończeniu świadczenia usług związanych z przetwarzaniem danych osobowych, podmiot przetwarzający usuwa lub zwraca ci wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.	
Zadbaj o odpowiednią formę umowy	
Sporządź umowę powierzenia przetwarzania danych osobowych w formie pisemnej. Możesz wybrać formę elektroniczną.	

Ponadto należy opracować wykaz wszystkich podmiotów, którym powierzasz przetwarzanie danych wraz z opisem celu, dla którego do tego przetwarzania dochodzi. Wystarczy prosta tabelka z odpowiednimi kolumnami (zob. wzór 6).

Wzór 6. Wykaz podmiotów, którym powierzono przetwarzanie danych osobowych

Nazwa podmiotu	
Cel powierzenia	
Zakres powierzonych danych, wykaz danych	
Czy zawarto umowę powierzenia	

NOWA POLITYKA BEZPIECZEŃSTWA I INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI

W kolejnym kroku warto pomyśleć o przygotowaniu dokumentacji, która będzie opisywać procedury postępowania z danymi osobowymi, jakie zachodzą w bibliotece. Chodzi o wskazanie m.in.:

- w jakich miejscach dochodzi do przetwarzania danych;
- kto ma dostęp do danych;
- jakie zastosowano środki w celu ochrony danych osobowych.

Nie musi być to żaden formalny dokument. W RODO znajdziemy jedynie wzmiankę, że można to robić za pomocą odpowiednich polityk. Samemu należy podjąć decyzję, jak takie polityki mają wyglądać i jak bardzo szczegółowe informacje zawierać. Taką decyzję należy podjąć, kierując się podstawową zasadą, na jaką kładzie nacisk RODO – wdrożenie odpowiednich rozwiązań związanych z ochroną danych osobowych. Odpowiednich do skali, celów, charakteru, zakresu i kontekstu przetwarzania danych.

Tworząc taką dokumentację, kluczowe jest, by zastanowić się nad środkami ochrony danych. Te środki mają być takie, by zapewnić danym bezpieczeństwo (art. 32 RODO). Chodzi o to, by dane nie wyciekły, by nie uzyskał do nich dostęp nikt nieuprawniony, by nikt ich nie skasował, zmodyfikował itp. Być może stosowane dotychczas zabezpieczenie techniczne i organizacyjne wystarczą. Warto rozważyć wdrożenie dodatkowych środków, które poprawią bezpieczeństwo ochrony danych. Gdy jakieś informacje w tych dokumentach nie odpowiadają rzeczywistości, należy je poprawić. Jeżeli nie ma polityki bezpieczeństwa i instrukcji, warto przygotować choćby jeden dokument opisujący postępowanie z danymi osobowymi w jednostce.

Masz pytania do prawnika?
Wyślij je e-mailem na adres
bibliotekapubliczna@sukurs.edu.pl.
Odpowiedzi na wybrane pytania zostaną opublikowane w kolejnych numerach
„Biblioteki Publicznej”.

UPOWAŻNIENIA DO PRZETWARZANIA DANYCH

Jeżeli chodzi o:

- ewidencję osób upoważnionych;
- wzór upoważnienia,

w tych dokumentach nie trzeba nic zmieniać. Oczywiście jeśli jednostka upoważnia te same osoby do przetwarzania danych osobowych. Jeżeli jednak w treści odnoszą się do art. 37 ustawy o ochronie danych osobowych, warto to poprawić i wykreślić.

ZGŁOSZENIE NARUSZENIA DANYCH OSOBOWYCH

Kolejną nowością RODO jest obowiązek zgłaszania naruszeń ochrony danych osobowych. Biblioteka będzie miała obowiązek zgłaszania wszelkich naruszeń bezpieczeństwa danych osobowych w czasie do 72 godzin od naruszenia, bezpośrednio do właściwego organu nadzoru – Prezesa UODO (art. 33 RODO). Chodzi o sytuacje, gdy dane, które gromadzi jednostka, wyciekają w niewiadomych okolicznościach, uzyskuje do nich dostęp ktoś nieuprawniony itd. Każdy taki incydent powinien być wyłapany, zewidencjowany i zaraportowany. Wszystko po to, być w stanie w ciągu 72 godzin podjąć decyzję, czy zgłaszać naruszenie do organu nadzorczego, czy nie. Do organu nadzorczego nie trzeba zgłaszać naruszeń, jeśli dyrektor lub inspektor ochrony danych oceni, że jest mało prawdopodobne, by skutkowały one ryzykiem naruszenia praw lub wolności osób fizycznych.

UWAGA! Trwają prace legislacyjne, które upoważnią obecnego RODO do stworzenia systemu, w którym będzie trzeba zgłaszać naruszenie. RODO określa minimum informacji, które powinny znaleźć się w zgłoszeniu naruszenia organowi nadzorczemu. Zgodnie z nimi zgłoszenie musi:

- opisywać charakter naruszenia, 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;
- opisywać możliwe konsekwencje naruszenia;
- opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

KOMUNIKAT O NARUSZENIU OCHRONY DANYCH

Zgodnie z RODO (art. 34) o naruszeniu ochrony danych trzeba zawiadomić osoby, których dane dotyczą. W przypadku bibliotek publicznych ten obowiązek został ograniczony w nowym przepisach dotyczących ochrony danych w ustawie o bibliotekach. Przepisy te są jeszcze na etapie prac legislacyjnych. Wystarczy, że administrator danych zamieści na swojej internetowej stronie podmiotowej lub w BIP komunikat o zaistniałym naruszeniu nie później niż 72 godziny od stwierdzenia naruszenia (może to robić IOD) (zob. wzór 7).

Wzór 7. Komunikat o naruszeniu ochrony danych

Komunikat o naruszeniu ochrony danych z dnia	
Charakter naruszenia ochrony danych	
Kategoria i przybliżona liczba osób, których dane dotyczą	
Liczba wpisów, których dotyczy naruszenie	
Możliwe konsekwencje naruszenia ochrony danych	
Środki zastosowane lub proponowane w celu zaradzenia naruszenia ochrony danych osobowych, w tym zastosowane środki w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych	

.....

podpis dyrektora w imieniu administratora danych

KLAUZULE INFORMACYJNE

Obowiązek informacji jest znacznie szerszy niż obecnie. Warto porównać art. 13 i 14 RODO i art. 24, 25 obecnej ustawy o ochronie danych osobowych. Wzór zawiera nie wszystkie informacje, jakich wymaga RODO. Jeżeli dane osobowe czytelnika czy innych osób będą przekazywane do państwa trzeciego lub organizacji międzynarodowej, trzeba zmodyfikować wzór o wymagania z RODO – art. 13 ust. 1 pkt f. To samo dotyczy sytuacji, gdy biblioteka przetwarza dane pozyskane z innych źródeł niż od osoby, której dane dotyczą – art. 14 RODO (zob. wzór 8). Warto śledzić stronę www.giodo.gov.pl; być może do 25 maja 2018 r. pojawią się jakieś wytyczne co do formy i wzoru takiej klauzuli informacyjnej.

Przekazywana informacja w swojej treści, poza jej prostotą i jasnością przekazu, ma być zwięzła, przejrzysta, zrozumiała i dostępna w łatwej formie.

Wzór 8. Klauzula informacyjna

Zgodnie z art. 13 ust. 1 i ust. 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. informuję, iż:

1. administratorem Pana/i danych osobowych jest ... (nazwa biblioteki) z siedzibą w ... (adres);
2. inspektorem ochrony danych w ... (nazwa biblioteki) jest Pan/i (imię i nazwisko inspektora) ... (e-mail lub inne dane kontaktowe) ...;
3. Pana/i dane osobowe przetwarzane będą w celu ... (należy podać cel przetwarzania) na podstawie ... (należy podać podstawę prawną przetwarzania np. art. 6 ust 1 pkt a/b/c/d/e/f RODO);
4. odbiorcą Pana/i danych osobowych będą ... (można wymienić kategorię odbiorców, o ile istnieją; jeżeli nie ma, piszemy, że dane nie będą udostępnianie innym odbiorcom);
5. Pana/i dane osobowe będą przechowywane przez okres ... (jeżeli nie ma możliwości wskazania okresu przechowywania, należy podać kryterium ustalania tego okresu np. do czasu wyłonienia zwycięzcy konkursu, do czasu zakończenia rekrutacji itd.);
6. posiada Pan/i prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnię-

cia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania (jeżeli przetwarzanie odbywa się na podstawie zgody), którego dokonano na podstawie zgody przed jej cofnięciem;
7. ma Pan/i prawo wniesienia skargi do GIODO, gdy uzna Pan/i, iż przetwarzanie danych osobowych Pana/i dotyczących narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.;
8. podanie przez Pana/ią danych osobowych jest ... (wybrać odpowiednio: wymogiem ustawowym/ warunkiem umownym/ warunkiem zawarcia umowy). Jest Pan/i zobowiązany do ich podania, a konsekwencją niepodania danych osobowych będzie ... (jeżeli osoba, której dane dotyczą, jest zobowiązana do ich podania, należy wskazać ewentualne konsekwencje niepodania danych);
9. Pana/i dane będą przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania. Zautomatyzowane podejmowanie decyzji będzie odbywało się na zasadach ... , konsekwencją takiego przetwarzania będzie ... (należy wskazać istotne informacje o zasadach zautomatyzowanego podejmowania decyzji oraz informacje o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą, jeżeli jest prowadzone).

JAK ZAPOZNAĆ PRACOWNIKÓW Z RODO?

Najlepiej zorganizować wewnętrzne szkolenie, na którym dyrektor przedstawi nowe rozwiązania, powie co się zmieni, jakie będą nowe obowiązki, przedstawi inspektora ochrony danych, itd (zob. wzór 9).

ŹRÓDŁO:

- projekt ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych (z 12 września 2017 r.).

PODSTAWA PRAWNA:

- rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (Dz.Urz. UE. L nr 119, str. 1).

DARIUSZ **SKRZYŃSKI**
prawnik, specjalista z zakresu prawa oświatowego, prawa pracy i prawa autorskiego
www.eduprawnik.pl

Wzór 9. Lista kontrolna – jak zapoznać pracowników z RODO

Sprawdź, czy pracownicy są świadomi zmian wynikających z RODO	Tak/Nie
Upewnij się, że pracownicy w bibliotece są świadomi zmian wprowadzanych przez ogólne rozporządzenie o ochronie danych, jakie nastąpią od 25 maja 2018 r. (tzw. RODO).	
Ustal, czy rozumieją skalę wyzwań, jakie niesie wykazanie zgodności z ogólnym rozporządzeniem o ochronie danych.	
Sprawdź, czy zespół ds. zmian w ochronie danych zidentyfikował już obszary, które koniecznie wymagają zmian w związku z ogólnym rozporządzeniem o ochronie danych.	
Zaangażuj administratora bezpieczeństwa informacji w podnoszenie wiedzy osób przetwarzających dane osobowe na temat RODO	
Jeśli w bibliotece został powołany administrator bezpieczeństwa informacji (ABI), powinien on już teraz podnosić wiedzę wszystkich osób uczestniczących w procesach przetwarzania danych osobowych, przygotowując ich tym samym do stosowania nowego prawa ochrony danych osobowych.	
Rozważ zasadność udziału osób przetwarzających dane osobowe w zewnętrznych szkoleniach.	
Możesz skorzystać z zewnętrznych firm, które pomogą ci przygotować pracowników do przetwarzania danych według zasad ogólnego rozporządzenia o ochronie danych.	
Zacznij przygotowania do ogólnego rozporządzenia o ochronie danych już teraz	
Nie zostawiaj na ostatnią chwilę przygotowania do stosowania ogólnego rozporządzenia o ochronie danych, w tym zapoznania pracowników przetwarzających dane osobowe i kadry kierowniczej z tymi przepisami.	
Wykorzystaj czas, który pozostał do momentu rozpoczęcia stosowania ogólnego rozporządzenia o ochronie danych, na rzetelny przegląd wszystkich prowadzonych czynności przetwarzania danych osobowych, tak by 25 maja 2018 r. móc już wykazać zgodność z nowymi unijnymi przepisami.	
Przygotowując się do stosowania ogólnego rozporządzenia o ochronie danych, możesz posiłkować się wytycznymi przygotowanymi przez Generalnego Inspektora Ochrony Danych Osobowych i Grupę Roboczą art. 29.	