

RODO w projektach Aktywni Obywatele

Katarzyna Sadło

Nie dać się zwariować

To NIE są wymogi RODO!



ZARZĄDZENIE OCHRONA DANYCH OSOBOWYCH

W związku wejściem w życie w dniu 25 maja 2018 r. z rozporządzenia Parlamentu Europejskiego i Rady (UE) o ochronie danych osobowych z dnia 27 kwietnia 2016 r. - RODO (Dz. U. UE. L. z 2016 r. Nr 119) z dniem 4 czerwca 2018 r. wprowadza się co następuje:

Zobowiązuje się Personel Przedszkola, Współpracowników, Rodziców/Prawnych Opiekunów, wszelkie inne osoby do zastosowania się do poniższych zasad Ochrony Danych Osobowych i Pseudonimizacji:

1. Dane Osobowe Dzieci, Rodziców/Prawnych Opiekunów, Współpracowników i innych osób

Nie posługiwane się na terenie Przedszkola Danymi w tym również nazwiskiem.

W celu identyfikacji proszę używać danych pseudonimizowanych:

nr karty, nr ewidencyjny, inicjały.

2. Rzeczy Osobiste

Nie podpisywać żadnych rzeczy osobistych imieniem i nazwiskiem.

Takie przedmioty nie będą przyjmowane do Przedszkola i zwracane lub niezwłocznie niszczone.

Do opisu proszę używać danych powyżej: nr karty, nr ewidencyjny, inicjały.

3. Listy Obecności

Podpisywać listy obecności nieczytelnym podpisem.

4. Korespondencja, Składanie Dokumentów

Składanie wszelkich dokumentów czy korespondencji, zawierających dane osobowe, w tym podań, opinii, orzeczeń, upoważnień itp. w:

a. formie papierowej za pośrednictwem poczty lub kuriera, listem poleconym. Kopertę proszę oznaczyć nr ewidencyjnym dziecka.

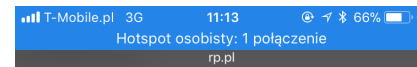
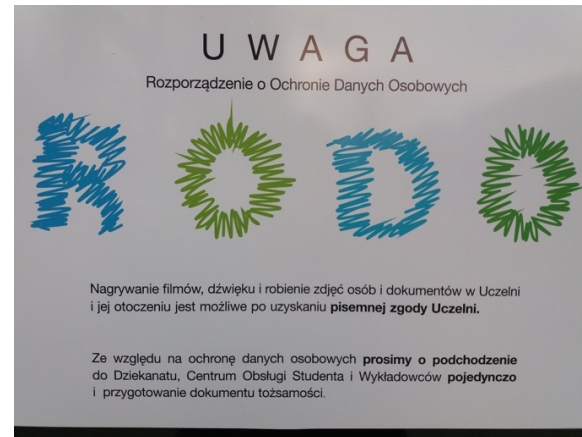
b. formie papierowej w placówce w zaklejonej kopercie adresowanej do Dyrektora Przedszkola. Kopertę proszę oznaczyć nr ewidencyjnym dziecka.

c. jeżeli korespondencja wymaga potwierdzenia jej przyjęcia przez Przedszkole, proszę o jej składanie bezpośrednio na ręce Dyrektora Przedszkola ds. Pedagogicznych, lub przesłanie listem poleconym za pośrednictwem poczty.

Do realizacji powyższego Zarządzenia zobowiązuje Kierownika Placówki/Dyrektora ds. Pedagogicznych.

29 sierpnia 2018 r.

Dyrektor Przedszkola



Przykładowo w firmie Jana Kowalskiego prowadzącego zakład stolarski będą inne ryzyka, a inne w dużej spółce handlowej – wskazuje adwokat. - W przypadku wizytówek większym problemem jest realizacja obowiązku informacyjnego wobec osoby, od której otrzymujemy wizytówkę, niż sposób jej zabezpieczenia – podkreśla ekspert.

Podstawowe definicje

Dane osobowe

- 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.

Dane osobowe wrażliwe

- Pochodzenie rasowe lub etniczne,
- Poglądy polityczne,
- Przekonania religijne lub światopoglądowe,
- Przynależność do związków zawodowych,
- Dane dotyczące zdrowia,
- Dane dotyczące seksualności lub orientacji seksualnej,
- Dane genetyczne,
- Dane biometryczne.

Przetwarzanie danych

- Operacje lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie 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;

Profilowanie

- dowolna forma **zautomatyzowanego** przetwarzania danych osobowych, która polega na **wykorzystaniu danych osobowych do oceny niektórych czynników osobowych** osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

Proces przetwarzania danych

Administrator („gospodarz” procesu)

- osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi (współadministratorami) **ustala cele i sposoby przetwarzania danych osobowych;**
- administratorów może być kilku – są wtedy współadministratorami;
- w przypadku osoby prawnej – **administratorem jest ta osoba prawna** jako podmiot (nie zarząd, czy konkretny pracownik);

Procesor (podmiot przetwarzający)

- Przetwarza dane osobowe **w imieniu administratora na podstawie umowy powierzenia przetwarzania** danych osobowych np.:
 - biuro rachunkowe prowadzące rozliczenia z kontrahentami,
 - podwykonawca prowadzący działania z wykorzystaniem danych osobowych,
 - podmiot prowadzący ewaluację,
 - firma hostująca bazę danych,
- Jeśli umowa powierzenia przetwarzania danych zezwala – procesor może podpowierzyć przetwarzanie danych podprocesorowi.

Umowa powierzenia przetwarzania

- określa przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora,
- zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy,
- jeżeli podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają te same obowiązki ochrony danych jak w umowie między administratorem a podmiotem przetwarzającym,
- jeżeli ten inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na pierwotnym podmiocie przetwarzającym.

Odbiorca danych

- Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, **któremu ujawnia się dane osobowe.**
- Nie są uznawane za odbiorców organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem UE lub prawem państwa członkowskiego.

W projektach Programu Aktywni Obywatele

- **Administrator** – Grantobiorca (samodzielnie lub wspólnie z Partnerami projektu),
- **Procesor** – np. biuro rachunkowe Grantobiorcy, podmioty realizujące na jego rzecz działania z wykorzystaniem danych,
- **Odbiorca** – Grantodawca i podmioty działające w jego imieniu,

Obowiązki Grantobiorcy

- Przetwarzanie danych w projekcie zgodnie z RODO i przepisami krajowymi,
- Wdrożenie środków zapewniających poziom bezpieczeństwa adekwatny do zakresu danych i celów ich przetwarzania,
- Przechowywanie dokumentacji projektu przez okres obowiązywania umowy grantowej, a po jej zakończeniu przez okres 3 lat od zakończenia programu rozumianego jako przyjęcie przez BMF końcowego sprawozdania z realizacji Programu.

Obowiązki Grantobiorcy

- W przypadku upowszechniania wizerunku swoich przedstawicieli, w tym koordynatorów Projektu i innych osób zaangażowanych w jego realizację, a także uczestników i uczestniczek Projektu, Grantobiorca musi uzyskać od tych osób stosowne zezwolenia,
- Zezwolenia te muszą zawierać także zgodę na upowszechnianie ich wizerunku przez Operatora do celów informowania o Programie,

Zasady przetwarzania danych

Zasada ograniczenia celu

- Dane osobowe muszą być **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 za niezgodne z pierwotnymi celami;
- *Jaki jest cel(e) przetwarzania poszczególnych danych w Twoim projekcie?*

Zasada minimalizacji danych

- Przetwarzane dane osobowe muszą być **adekwatne, stosowne** oraz **ograniczone do tego, co niezbędne do celów**, w których są przetwarzane.
- *Jakie dane osobowe są absolutnie niezbędne do realizacji celu?*
- *Z jakich danych możesz bez strat dla innowacji zrezygnować?*

Zasada ograniczenia przechowywania

- Dane osobowe mogą być 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;
- *Jak długo musisz przechowywać dane?*
- *Jak długo będą Ci potrzebne w celach, dla jakich je zbierasz?*

Zasada legalności i przejrzystości

- Dane osobowe muszą być przetwarzane **zgodnie z prawem**, rzetelnie i **w sposób przejrzysty dla osoby**, której dane dotyczą.
- *Jak się upewnisz, że osoby, których dane przetwarzasz rozumieją dlaczego i jak to robisz, oraz jakie są ich prawa?*
- *Jaki będzie adekwatny sposób spełniania obowiązku informacyjnego?*

Zasada integralności i poufności

- Dane osobowe muszą być 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;
- *Jak będziesz przechowywać dane osobowe?*
- *Jak zabezpieczysz dane osobowe przechowywane w papierze i elektronicznie?*

Podstawy prawne przetwarzania danych

Zgoda osoby (art. 6 ust 1a/art. 9 ust 2a)

- Zgoda to **dobrowolne, konkretne, świadome i jednoznaczne** okazanie woli w formie oświadczenia lub wyraźnego działania potwierdzającego,
- Zgoda może być odwołana w dowolnym momencie a dane usunięte na żądanie osoby, której dotyczą,
- Zgoda jest podstawą prawną przetwarzania danych np. kandydatów w rekrutacji, osób zapisujących się na newslettera oraz innych beneficjentów – ale tylko wtedy, gdy organizacja będzie mogła usunąć ich dane w dowolnym momencie, jeśli wycofają zgodę.

Kiedy nie prosić o zgodę...

Zgoda na przetwarzanie danych osobowych

Ja niżej podpisany/a wyrażam zgodnie z art. 7 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z 27 kwietnia 2016 r. tzw. RODO* wyraźną i dobrowolną zgodę na przetwarzanie danych osobowych moich oraz małoletniego dziecka przez

Specjalistyczny Gabinet

Kraków ('Gabinet')

w celu udokumentowania stanu zdrowia oraz udzielonych świadczeń zdrowotnych, komunikacji korzystania z usług medycznych, a także na otrzymywanie za pośrednictwem telefonii komórkowej i/lub poczty elektronicznej informacji dotyczących planowanych wizyt, jak również informacji o medycznej działalności Gabinetu.

Jednocześnie oświadczam, że moja zgoda spełnia wszystkie warunki o których mowa w art. 7 RODO, tj. przysługuje mi możliwość jej wycofania w każdym czasie, zapytanie o zgodę zostało mi przedstawione w wyraźnej i zrozumiałej formie oraz poinformowano mnie o warunku możliwości jej rozliczalności.

Zostałem/zostałam również poinformowany/a o tym, że dane zbierane są przez Gabinet, o celu ich zbierania, dobrowolności podania, prawie wglądu i możliwości ich poprawiania oraz że dane te nie będą udostępniane innym podmiotom, za wyjątkiem podmiotów wykonujących na rzecz Gabinetu usługi związane z medyczną działalnością Gabinetu oraz o tym, że podanie danych osobowych gromadzonych w dokumentacji medycznej przez Gabinet, zgodnie z odrębnymi przepisami, jest obowiązkowe.

Kiedy można prosić o zgodę...

 **frso** fundacja rozwoju społeczeństwa obywatelskiego

[O nas](#) [Działalność](#) [Oferta](#) [Publikacje](#) [Kontakt](#)

Klauzule

Wyrażam zgodę na przetwarzanie moich danych osobowych zawartych w formularzu zgłoszeniowym w celu przeprowadzenia rekrutacji do programu szkoleń dla Doradców Lokalnych. Administratorem danych jest Fundacja Rozwoju Społeczeństwa Obywatelskiego, z siedzibą w Warszawie (03-717), ul. Kłopotowskiego 6 m 59/60. Zostałam/em poinformowana/y o przysługującym mi prawie do odwołania zgody w dowolnym momencie, oraz o tym, że takie odwołanie nie wpłynie na zgodność z prawem przetwarzania, którego dokonano przez tym odwołaniem. Dane będą przetwarzane do czasu wycofania przeze mnie zgody na to przetwarzanie, planowany termin usunięcia danych osób nieprzyjętych do programu to 1 miesiąc po ostatecznym zakończeniu procesu rekrutacji. W trakcie trwania rekrutacji dane mogą zostać udostępnione partnerowi programu – Fundacji Akademii Rozwoju Filantropii w Polsce, oraz fundatorowi programu – Polsko-Amerykańskiej Fundacji Wolności. Przysługuje mi prawo dostępu do treści moich danych, ich sprostowania, usunięcia, ograniczenia przetwarzania, a także prawo do przenoszenia danych. W przypadku przetwarzania moich danych niezgodnie z prawem przysługuje mi prawo do wniesienia skargi do Urzędu Ochrony Danych Osobowych. Moje dane nie będą podlegały profilowaniu, nie będą też przekazywane do państw trzecich ani organizacji międzynarodowych. Podanie danych jest dobrowolne, ale odmowa ich podania uniemożliwia udział w rekrutacji (pole wymagane) *

☐ Tak

Zgoda na przesyłanie materiałów informacyjnych FRSO

☐ Tak
☐ Nie

Oświadczam, że zapoznałam/em się z Regulaminem cyklu szkoleń dla Doradców Lokalnych i zobowiązuje się do jego przestrzegania (pole wymagane) *

☐ Tak

Deklaruję udział w 4 szkoleniach w pełnym wymiarze czasu (pole wymagane) *

☐ Tak

Zobowiązuję się do zrealizowania nieodpłatnie 64 godzin poradnictwa dla organizacji pozarządowych w ramach działalności delegującej mnie organizacji (pole wymagane) *

☐ Tak

Zobowiązuję się do poinformowania FRSO w przypadku niemożności udziału w zajęciach z powodów losowych, nie później niż na 3 dni przed rozpoczęciem szkolenia. W przypadku niezgłoszonej i nieusprawiedliwionej nieobecności zobowiązuję się pokryć poniesione przez Fundację koszty mojego zakwaterowania i wyżywienia w czasie szkolenia (pole wymagane) *

☐ Tak

Zachowaj

Umowa z osobą (art. 6 ust 1b)

- Przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy,
- Podstawa prawna przetwarzania danych pracowników, zleceniobiorców, wolontariuszy, stypendystów, kontrahentów oraz innych osób, z którymi łączy nas umowa,

Prawny obowiązek (art. 6 ust 1c)

- Przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze,
- Podstawa prawna przetwarzania danych do którego jesteśmy zmuszeni przepisami, w innowacji może to dotyczyć np. personelu pracującego z dziećmi, a także danych które mamy obowiązek przechowywać nawet po wygaśnięciu umowy łączącej nas z osobą (np. dane byłych pracowników, byłych zleceniobiorców)

Prawnie uzasadniony interes (art. 6 ust 1f)

- Przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem,
- W projektach to najczęściej podstawa przetwarzania danych beneficjentów - prawnie uzasadnionym interesem jest bowiem konieczność rozliczenia umowy z grantodawcą,
- To także podstawa prawna działań marketingowych, promocyjnych, fundraisingowych, obrony przed roszczeniami i dochodzenia roszczeń, zapewnienia bezpieczeństwa (np. monitoring wizyjny).

Obowiązki administratora danych

- Ustalenie odpowiedniej podstawy prawnej, celów i sposobów przetwarzania,
- Przeprowadzenie analizy ryzyka i zastosowanie adekwatnych środków bezpieczeństwa,
- Nadawanie upoważnień do przetwarzania przed dopuszczeniem do danych,
- Zawieranie umów powierzenia z procesorami,
- Spełnianie obowiązku informacyjnego i realizacja praw osób,
- Rejestrowanie czynności przetwarzania,
- Dokumentowanie i zgłaszanie naruszeń,

Rozpowszechnianie wizerunku

Prawo autorskie (art. 81)

1. Rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej. W braku wyraźnego zastrzeżenia zezwolenie nie jest wymagane, jeżeli osoba ta otrzymała umówioną zapłatę za pozowanie.
2. Zezwolenia nie wymaga rozpowszechnianie wizerunku:
 - 1) osoby powszechnie znanej, jeżeli wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych;
 - 2) osoby stanowiącej jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza.

Zgoda na wykorzystanie wizerunku

- Wskazanie celu, w jakim może być wykorzystany
- Wskazanie podmiotów, którym zgody udzielono
- Informacja o dobrowolności wyrażenia zgody
- Informacja o prawie do wycofania zgody

Obowiązki Administratora

Upoważnienie do przetwarzania

Upoważniam Jana Kowalskiego do przetwarzania danych osobowych, których administratorem jest **Fundacja X**.

Zobowiązuję Jana Kowalskiego do przestrzegania obowiązujących w **Fundacji X** zasad bezpiecznego przetwarzania danych osobowych, oraz powszechnie obowiązujących przepisów prawa.

Upoważnienie wydaje się na czas nieoznaczony.

Data, podpis

Oświadczenie upoważnionego

Oświadczam, że zapoznałem się z przepisami powszechnie obowiązującymi dotyczącymi ochrony danych osobowych, w tym z RODO, a także z obowiązującymi w **Fundacji X** opisem technicznych i organizacyjnych środków zapewniających ochronę i bezpieczeństwo przetwarzania danych osobowych i zobowiązuję się do przestrzegania zasad przetwarzania danych osobowych określonych w tych dokumentach.

Zobowiązuję się do zachowania w tajemnicy przetwarzanych danych osobowych, z którymi zapoznałem się oraz sposobów ich zabezpieczenia, zarówno w okresie trwania umowy jak również po ustaniu stosunku prawnego łączącego mnie z **Fundacją X**.

Data, podpis

Analiza ryzyka

Analiza ryzyka

Jakie przeszkody musi pokonać ktoś, aby „dobrać się” do danych:

- gdy jesteście w swojej siedzibie
- gdy w siedzibie nikogo nie ma
- przez internet

Analiza ryzyka

- Co złego się może stać?
- Jakie jest prawdopodobieństwo, że się stanie?
- Jakie będą skutki?
- Jak zmniejszyć prawdopodobieństwo i/lub skutki?

Analiza ryzyka

- Określenie i opis operacji na danych i rodzaju przetwarzanych danych
- Analiza konieczności ich prowadzenia i adekwatności przetwarzanych danych
- Identyfikacja stosowanych środków bezpieczeństwa
- Lista możliwych niebezpieczeństw (wewnętrznych i zewnętrznych, umyślnych i nieumyślnych)
- Ocena prawdopodobieństwa ich wystąpienia
- Identyfikacja możliwych skutków dla osób, których dane dotyczą
- Działania zaradcze (minimalizacja ryzyka)

Analiza ryzyka

Prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, należy określić poprzez **odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych**. Ryzyko należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko.

Przykłady sytuacji, w których dochodzi do naruszenia praw i wolności osób, których dane są przetwarzane

Przykład 1. W wyniku włamania na niewystarczająco zabezpieczony serwer poczty elektronicznej korespondencja prywatna użytkownika X z osobą Y została pozyskana przez osobę Z, która wykorzystała zdobyte informacje do czerpania korzyści finansowych, szantażując adresata i nadawcę wiadomości upublicznieniem informacji – *naruszenie prawa do ochrony danych osobowych, prawa do prywatności oraz wolności i prawa do tajemnicy komunikowania się.*

Przykład 2. W wyniku słabo zabezpieczonej ciągłości działania systemu bankowego użytkownik X na skutek niedostępności tego systemu nie mógł dokonać transakcji finansowej na giełdzie w określonym czasie – *naruszenie prawa do ochrony danych osobowych oraz prawa własności.*

Przykład 3. Firma ubezpieczeniowa X w wyniku nabycia informacji o rodzajach kupowanych przez swoich klientów produktów żywnościowych w jednej z sieci supermarketów dokonała analizy tych danych i podniosła składkę ubezpieczenia dla osób, z których profilu można było wywnioskować nieprawidłowe odżywianie się – *naruszenie prawa do prywatności, prawa do ochrony danych osobowych, w tym prawa do niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu.*

			SKUTEK				
			Bardzo niski	Niski	Średni	Wysoki	Bardzo wysoki
			1	2	3	4	5
PRAWDOPODOBIEŃSTWO	Prawie pewne	5	Ś	W	K	K	K
	Prawdopodobne	4	Ś	W	W	K	K
	Możliwe	3	N	Ś	W	W	K
	Mało prawdopodobne	2	N	Ś	Ś	W	W
	Rzadkie	1	N	N	Ś	W	W

	Poziom ryzyka	Opis działania
	Niski (N)	Poziom ryzyka akceptowany – działania podejmowane w zależności od wymaganych nakładów
	Średni (Ś)	Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga okresowego monitorowania
	Wysoki (W)	Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga stałego monitorowania
	Krytyczny (K)	Poziom ryzyka nietolerowany – wymaga natychmiastowego działania

Tabela 3. Przykładowa macierz ryzyka



Jak stosować podejście oparte na ryzyku?

37

Rodzaj operacji przetwarzania danych	Zidentyfikowane zagrożenia	Poziom ryzyka naruszenia praw i wolności	Decyzja	Uzasadnienie akceptacji wyliczonego poziomu ryzyka
Przechowywanie elektronicznej dokumentacji medycznej	Utrata dostępności danych w przypadku awarii nośnika danych.	Niski (uzasadnienie: wdrożono system kopii zapasowej w trybie ciągłym ze względu na niezbędność ciągłego dostępu do danych pacjentów).	Akceptacja ryzyka	Zastosowanie systemu kopii zapasowej w trybie ciągłym, w architekturze systemów pracujących równolegle, zapewniających ciągłość dostępu na poziomie wysokim.

Tabela 5. Przykład tabeli operacji przetwarzania z oceną ryzyka.

Środki bezpieczeństwa

- Organizacyjne (procedury)
- Fizyczne (zabezpieczenia techniczne)
- Informatyczne (zabezpieczenia systemu)

Klauzula informacyjna

Zawartość klauzuli informacyjnej

- Nazwa i dane kontaktowe administratora oraz Inspektora Ochrony Danych (jeśli został powołany),
- Cel przetwarzania,
- Podstawa prawna przetwarzania,
- Okres przez jaki dane będą przechowywane lub kryteria ustalenia tego okresu,
- Informacje o odbiorcach lub kategoriach odbiorców,
- Informacja o przysługujących osobie prawach dotyczących jej,

Zawartość klauzuli informacyjnej

- informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą
- jeśli dane zostały pozyskane od osoby innej, niż osoba której dane dotyczą - źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych
- informacja, 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
- 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,

Prawa osoby

Prawa osób

Administrator bez zbędnej zwłoki – **w terminie miesiąca** – udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań.

Jeżeli żądania są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może: pobrać rozsądną opłatę, albo odmówić podjęcia działań w związku z żądaniem.

Prawa osób

- Dostępu do treści danych
- Sprostowania danych
- Prawo do usunięcia danych (z zastrzeżeniami!)
- Przenoszenia danych (tylko jeśli zgoda lub umowa są podstawą)
- Ograniczenia przetwarzania
- Wycofania zgody (tylko jeśli zgoda jest podstawą)
- Wniesienia sprzeciwu (tylko jeśli prawnie uzasadnione interesy są podstawą)
- Wniesienia skargi do PUODO

Prawo do bycia zapomnianym

Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli:

- Dane osobowe nie są już niezbędne do celów, w których zostały zebrane,
- Osoba, której dane dotyczą cofnęła zgodę,
- Osoba, której dane dotyczą wniosła uzasadniony sprzeciw wobec przetwarzania i nie istnieje żadna nadrzędna przesłanka,
- Dane osobowe były przetwarzane niezgodnie z prawem.

Rejestrowanie czynności przetwarzania

Rejestr czynności przetwarzania

Czynność przetwarzania - zespół 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 przypadku rekrutacji pracowników, jeden cel będzie obejmował wiele częściowych operacji niewymagających szczegółowego ich opisywania w rejestrze, takich jak. pozyskiwanie informacji o kandydatach z ofert nadesłanych w wyniku ogłoszenia, dokonywanie ich selekcji, uzyskiwanie dodatkowych informacji w ramach przeprowadzania wywiadów z wybranymi osobami, usunięcie danych osób, które nie zostały wskazane do zatrudnienia itp.

Rejestr czynności przetwarzania

- nazwa i dane kontaktowe administratora,
- cele przetwarzania,
- opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych,
- kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione,
- planowane terminy usunięcia poszczególnych kategorii danych
- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa,

Rejestr czynności przetwarzania

- nazwa i dane kontaktowe administratora,
- cele przetwarzania,
- opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych,
- kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione,
- planowane terminy usunięcia poszczególnych kategorii danych
- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa,

Postępowanie z naruszeniami

Definicja naruszenia

Naruszenie - 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.

Dokumentacja naruszeń

Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorcemu weryfikowanie przestrzegania przepisów.

Zgłaszanie naruszeń

- Administrator zgłasza naruszenie bez zbędnej zwłoki urzędowi ochrony danych osobowych – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Zgłoszenia dokonuje się na formularzu dostępnym na stronie UODO (www.Uodo.Gov.Pl)
- Jeśli jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, zgłoszenia się nie dokonuje.
- Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu, o ile nie zachodzą okoliczności zwalniające go z tego obowiązku.
- PUODO na podstawie uzyskanych informacji o naruszeniu może jednak nakazać zgłoszenie go osobie, której dane dotyczą.



Dziękuję za uwagę