Stołeczne Centrum Wspierania Organizacji Pozarządowych

System bezpłatnego wsparcia dla NGO

warszawa.ngo.pl

Jak stworzyć politykę danych osobowych (PDO)

Ekspertka: Justyna Bułdys

25.04.2018

Program

część 1.	Słowniczek pojęć i podstawy prawne
część 2.	Porównanie PBI i PDO
część 3.	Budowa i cechy PDO
część 4.	Jak korzystać z PDO

Słowniczek

Polityka danych osobowych - najważniejszy w organizacji dokument wewnętrzny regulujący przetwarzanie DO

Polityka prywatności - służy jako pomoc w zrozumieniu, jakie dane zbiera organizacja i w jakim celu oraz do czego je wykorzystuje; najczęściej publikowana na stronie internetowej

Słowniczek

Polityka bezpieczeństwa informacji - wskazuje środki bezpieczeństwa i procedury bezpiecznego przetwarzania informacji, w tym DO

Instrukcja zarządzania systemem informatycznym - opisuje korzystanie z systemu, w którym przetwarzane są DO z użyciem nowych technologii oraz istniejące zabezpieczenia

Słowniczek

Klauzula zgody - oświadczenie woli podmiotu DO, będące jednym z warunków legalności przetwarzania DO

Klauzula informacyjna - informacja Administratora Danych Osobowych skierowana do podmiotów DO dotycząca m.in. rodzaju DO oraz celu, sposobu i czasu ich przetwarzania

Słowniczek

Rejestr czynności przetwarzania - spis procesów mających miejsce w organizacji, podczas których przetwarzane są DO

Umowa powierzenia przetwarzania DO - umowa zawierana pomiedzy ADO a procesorem, który przetwarza dane w imieniu ADO i w tym samym celu (np. księgowośc zewnętrzna)

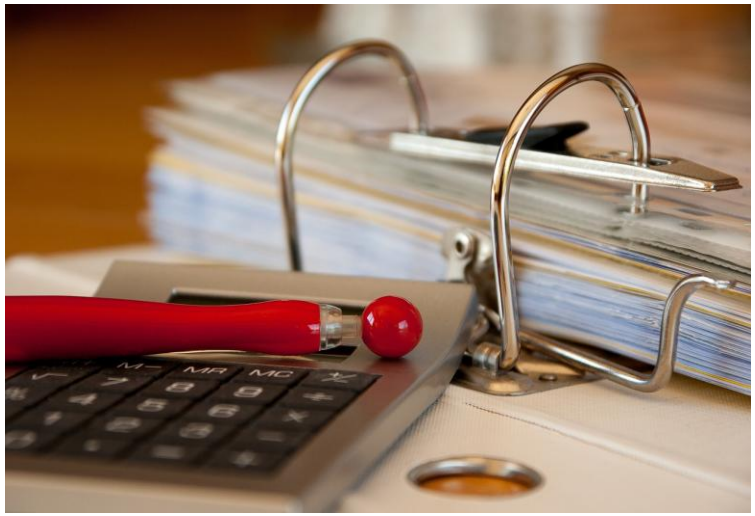
Słowniczek

Naruszenie w zakresie DO - incydent prowadzący do utraty atrybutów DO (np. brak podstawy do legalnego przetwarzania, wyciek danych)

Ocena skutków przetwarzania - analiza mająca na celu oszacowanie ryzyka utraty atrybutów DO w wyniku przetwarzania konkretnych kategorii DO przy wykorzystaniu konkretnych zasobów

Po co organizacji PDO?

- pozwala **uporządkować** aktywa, procesy i zagrożenia występujące w sytuacji przetwarzania DO
- **zwiększa świadomość** tego, co dzieje się w organizacji, wzmacniając poczucie pewności i spokoju
- **chroni** organizację w sytuacji incydentu lub kontroli



Podstawa prawna

- **Art. 24 ust. 1 RODO** „Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i **aby móc to wykazać**. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane."
- **Art. 24 ust. 2 RODO** „Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich **polityk ochrony danych**."

Porównanie PBI i PDO

	PBI wg uodo i rozp. o KRI	PDO wg rodo
wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe	V	V
wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	V	V (+ rejestr czynności)
opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	V	V

Porównanie PBI i PDO

	PBI wg uodo i rozp. o KRI	PDO wg rodo
sposób przepływu danych pomiędzy poszczególnymi systemami	V	V
określenia środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	V	V

Porównanie PBI i PDO

	PBI wg uodo i rozp. o KRI	PDO wg rodo
procedura **postępowania w przypadku wystąpienia naruszenia** – system reakcji na incydenty	-	V
ścieżka **postępowania w przypadku wystąpienia wniosku informacyjnego** od osoby, której dane dotyczą	-	V
ścieżka **postępowania w przypadku złożenia sprzeciwu** co do przetwarzania danych osobowych do celów marketingu bezpośredniego	-	V

Co jeszcze powinna zawierać PDO?

- uwzględnienie zasad **privacy by design** oraz **privacy by default**
- uwzględnienie prawa do **przenoszalności** danych oraz prawa do **zapomnienia**
- **ocenę skutków** dla przetwarzania DO

Co jeszcze powinna zawierać PDO?

► **załączniki** (wzory):

- Klauzula informacyjna stosowana w przypadku zbierania DO od osoby, której one dotyczą
- Klauzula informacyjna stosowana w przypadku zbierania DO nie od osoby, której one dotyczą
- Klauzula zgody
- Upoważnienie do przetwarzania DO
- Ewidencja osób upoważnionych do przetwarzania DO
- Umowa powierzenia przetwarzania DO
- Ocena skutków przetwarzania (jeśli jest)

Cechy PDO wg RODO

- zgodna z zasadą uwzględniania ochrony danych w fazie projektowania (privacy by design),
- zgodna z zasadą domyślnej ochrony danych (privacy by default),
- proporcjonalna w stosunku do czynności przetwarzania danych,
- napisana jasnym i przejrzystym językiem.

Cechy PDO wg RODO

- PDO można i należy aktualizować i dostosowywać w ramach **ciągłej analizy** działań organizacji.
- PDO nie tworzy się „do szuflady”. Po jej stworzeniu należy **zapoznać** z nią pracowników i **wdrożyć** do praktycznego stosowania.

4 kroki do aktualizacji PDO

1. **Zapoznaj się** z nowym prawem w zakresie ODO
2. Zrób **audyt** dotychczasowej dokumentacji
3. Oceń, co należy **zmienić**
4. **Wprowadź** aktualizacje i przeprowadź ponowne **szkolenie** dla pracowników

Rejestr czynności przetwarzania

Kogo NIE dotyczy:

administratorzy zatrudniający **mniej niż 250** pracowników, chyba że przetwarzanie danych przez te podmioty:

- może powodować **ryzyko naruszenia** praw i wolności osób, których dane dotyczą,
- nie ma charakteru sporadycznego,
- obejmuje **szczególne kategorie** danych osobowych,
- dotyczy danych na temat **wyroków** skazujących i naruszeń praw.

Rejestr czynności przetwarzania

Co zawiera (art. 30 RODO)

- imię i nazwisko lub nazwę oraz dane kontaktowe administratora, współadministratorów oraz inspektora ochrony danych, jesli jest powołany
- cel przetwarzania,
- opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych,
- kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub organizacjach międzynarodowych,

Rejestr czynności przetwarzania

- przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej,
- planowane terminy usunięcia poszczególnych kategorii danych,
- opis technicznych i organizacyjnych środków bezpieczeństwa mających zapewnić odpowiedni poziom bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

Najczęstsze błędy przy tworzeniu dokumentacji

- wzory dokumentów „z internetu”
- błędnie wskazany obszar przetwarzania
- niekompletne klauzule zgody i/lub informacyjne
- niekompletne ewidencje upoważnień
- nieaktualna dokumentacja
- brak szkoleń
- brak praktycznego wdrożenia PDO

Udostępnianie PDO

► **procesorom**, którym PDO jest niezbędna w związku z powierzeniem przetwarzania danych

► podmiotom, które wykażą, że na mocy przepisów prawa **są uprawnione** do ich uzyskania (kontrolorzy PUODO lub NIK, prokuratura, sądy)

Dokumentacja uzupełniająca

- IZSI
- oświadczenia o zachowaniu danych osobowych w poufności
- rejestr naruszeń
- dokumentacja wyznaczenia inspektora danych osobowych
- informacja o retencji danych (**uwaga!** zasada minimalizacji czasu - art. 5 ust. 1 lit. e RODO)

Dowiedz się więcej

- Nagrania oraz prezentacje z wcześniejszych webinariów SCWO:
  warszawa.ngo.pl/webinaria

- Pełna oferta i aktualności SCWO:
  warszawa.ngo.pl/scwo
  facebook.com/warszawa.ngo

Stołeczne Centrum Wspierania Organizacji Pozarządowych

SYSTEM BEZPŁATNEGO WSPARCIA DLA NGO

Projekt współfinansuje m.st.Warszawa

zakochaj się w Warszawie

Projekt „Stołeczne Centrum Wspierania Organizacji Pozarządowych" współfinansuje m.st. Warszawa.

warszawa.ngo.pl