

Technologia Infromacyjna i Prawo w służbie ochrony danych - #RODO2018

Jak RODO wpłynie na pracę działów HR – nowe obowiązki
pracodawców

Tomasz Pleśniak

A photograph of a brass padlock and a set of keys resting on a blue surface. In the background, a laptop keyboard is visible, with keys illuminated in a greenish-blue light. The overall scene is set against a dark blue background with a subtle grid pattern.

Kiedy można przetwarzać dane osobowe?

- **Przetwarzanie danych osobowych jest dopuszczalne jedynie w przypadkach określonych w art. 6 ust. 1 RODO:**
 - 1) osoba, której dane dotyczą wyraziła **zgode** na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów
 - 2) 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
 - 3) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze

Art. 22¹ Kodeksu pracy:

Pracodawca **ma prawo** żądać od osoby ubiegającej się o zatrudnienie podania danych osobowych obejmujących:

- 1) imię (imiona) i nazwisko;
- 2) imiona rodziców;
- 3) datę urodzenia (...)

Zasada rozliczalności

Pochodną rewolucyjnej zmiany jest wprowadzenie odpowiedzialności ADO za przestrzeganie podstawowych zasad przetwarzania danych osobowych, to jest:

- **zgodność z prawem, rzetelność i przejrzystość** dla osoby, której dane dotyczą
- **ograniczenie celu** – wyraźny, prawnie uzasadniony
- **minimalizacja danych** – w poprzednim stanie prawnym **adekwatność**
- **prawidłowość** – szybkie usuwanie nieprawidłowości
- **ograniczenie okresu przechowywania** – w tym prawo do bycia zapomnianym
- **integralność i poufność** – zabezpieczenie przed utratą, zniszczeniem

RODO przewiduje, że ADO musi być w stanie wykazać przestrzeganie powyższych zasad (zasada rozliczalności przetwarzania danych osobowych)

Risk-based approach – największe wyzwanie RODO

Odejście od formalnej ochrony danych osobowych – przedsiębiorca sam ocenia, jakie ryzyka są związane z przetwarzaniem przez niego danych osobowych i na tej podstawie opracowuje środki służące ochronie tych danych

*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***

Ocena przedsiębiorcy musi mieć **charakter ciągły** – uwzględniać zmiany powyższych aspektów!

*Jeżeli jest to **proporcjonalne w stosunku do czynności przetwarzania**, środki, o których mowa powyżej, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych*

Privacy by design / Privacy by default

- **Privacy by design** – obowiązek zapewnienia już w fazie projektowania nowej usługi/nowego towaru tak, aby spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą (w szczególności służyć to ma realizacji zasady minimalizacji danych)
- **Privacy by default** – ADO ma obowiązek wdrażania odpowiednich środków technicznych i organizacyjnych, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania

Nowe instytucje oraz zmiany wprowadzone przez RODO

NOWOŚCI

- **nowe podejście do ochrony danych osobowych (risk-based approach)**
- **zasada rozliczalności przetwarzania**
- **privacy by design/privacy by default**
- **wprowadzenie kar administracyjnych**
- raportowanie o własnych naruszeniach do organu nadzoru
- obowiązek posługiwania się prostym, jasnym i zrozumiałym językiem

ZMIANY

- rozszerzona formuła zgody na przetwarzanie danych
- rozszerzony zakres obowiązku informacyjnego
- rejestr czynności przetwarzania
- zmiana statusu ABI > IOD
- nowa instytucja kontrolująca UODO > PUODO
- zwiększenie uprawnień osób, których dane dotyczą

Operacje na danych osobowych pracowników

Dane osobowe pracowników:

- 1) pozyskujemy;
- 2) przetwarzamy (w tym **przechowujemy**);
- 3) Usuwamy (?)

Okres retencji – czy zawsze 50 lat?

Rejestr czynności przetwarzania danych

Obowiązek prowadzenia rejestru czynności danych nie ma zastosowania do przedsiębiorcy lub podmiotu zatrudniającego **mniej niż 250 osób**,

chyba że przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, **nie ma charakteru sporadycznego** lub **obejmuje szczególne kategorie danych osobowych** lub **dane osobowe dotyczące wyroków skazujących i naruszeń prawa**.

Zgoda pracownika

Zgoda pobierana od pracownika – projekt ustawy wprowadzającej RODO

- Art. 22². §1. Przetwarzanie przez pracodawcę innych danych osobowych niż wymienione w art. 221 §1 i 2 **jest dopuszczalne za zgodą osoby ubiegającej się o zatrudnienie lub pracownika i tylko wtedy, gdy jest to dla nich korzystne.**
- §2. Brak zgody, o której mowa w §1 lub jej wycofanie, **nie może być podstawą niekorzystnego traktowania osoby ubiegającej się o zatrudnienie lub pracownika, a także nie może powodować wobec nich jakichkolwiek negatywnych konsekwencji**, zwłaszcza nie może stanowić przyczyny uzasadniającej odmowę zatrudnienia, wypowiedzenie umowy o pracę lub jej rozwiązanie bez wypowiedzenia przez pracodawcę.
- §3. Przetwarzanie, o którym mowa w §1, dotyczy danych osobowych udostępnianych przez osobę ubiegającą się o zatrudnienie lub pracownika **na wniosek pracodawcy** lub danych osobowych **przekazanych pracodawcy z inicjatywy** osoby ubiegającej się o zatrudnienie lub pracownika.

Obowiązek informacyjny - porównanie

RODZAJ INFORMACJI	UODO	RODO
adres, pełna nazwa administratora danych osobowych	+	+
dane kontaktowe (np. mail, telefon)	-	+
dane kontaktowe inspektora ochrony danych	-	+
cel przetwarzania danych osobowych	+	+
podstawa przetwarzania danych osobowych wraz z ew. opisem prawnie uzasadnionych interesów realizowanych przez administratora	-	+
informacje o odbiorcach danych osobowych	+	+
informacje o zamiarze przekazania danych osobowych do państwa trzeciego	-	+
informacja o okresie przechowywania danych osobowych	-	+

Obowiązek informacyjny - porównanie

RODZAJ INFORMACJI	UODO	RODO
informacja o prawie dostępu do danych osobowych oraz ich sprostowania	+	+
informacja o prawie usunięcia danych osobowych lub ograniczenia przetwarzania, o prawie do wniesienia sprzeciwu oraz o prawie do przenoszenia danych	-	+
informacja o prawie do cofnięcia zgody na przetwarzanie danych	-	+
informacja o prawie do wniesienia skargi do organu nadzorczego	-	+
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	-	+
informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu	-	+

Zgłaszanie naruszenia ochrony danych osobowych

W przypadku naruszenia ochrony danych osobowych, **administrator** bez zbędnej zwłoki – w miarę możliwości, **nie później niż w terminie 72 godzin po stwierdzeniu naruszenia** – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to **skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych**. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się **wyjaśnienie przyczyn opóźnienia**.

Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych **bez zbędnej zwłoki zgłasza je administratorowi**.

**Max
72h**

Gdzie w tym całym procesie pracownik?

Nowe prawa = nowe wyzwania

Ograniczenie przechowywania – czyli pamiętaj o terminie ważności...

Prawo do bycia zapomnianym – czyli nigdy mnie tutaj nie było...

Prawo do przenoszenia danych – czyli pomóż mi przejść do konkurencji...

**Bardzo dziękujemy
za Państwa uwagę!**

Państwa osoba do kontaktu



Tomasz Pleśniak

Radca Prawny, Senior Associate

Rödl & Partner

ul. Św. Mikołaja 19

50-128 Wrocław

Tel: +48 (71) 60 60 000

Fax: +48 (71) 60 60 131

E-mail: tomasz.plesniak@roedl.pro