10 PRZYKAZAŃ RODO DLA PRACODAWCÓW

r.pr. Edyta Jagiełło

Ius Laboris Poland Global HR Lawyers
Raczkowski Paruch | 10 2007-2017

INFOR | WIDE AKADEMIA

Ważne zmiany!!!

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE („RODO”)

- 4 maja 2016 r. – publikacja w Dzienniku Urzędowym UE
- 24 maja 2016 r. – wejście w życie (20 dni od daty publikacji)
- 25 maja 2018 r. – stosowanie przepisów RODO w państwach Unii Europejskiej (tj. w terminie 2 lat licząc od 24 maja 2016 r.)
- Nowe przepisy będą stosowane także wobec przetwarzania danych osobowych zebranych przed wejściem w życie RODO

INFOR | WIDEO AKADEMIA

art. 88 RODO

- ust.1 Państwa członkowskie **mogą** zawrzeć w swoich przepisach lub w porozumieniach zbiorowych bardziej **szczegółowe przepisy mające zapewnić ochronę praw i wolności** w przypadku przetwarzania danych osobowych pracowników w związku z zatrudnieniem, (….)
- ust. 2 Przepisy te muszą obejmować odpowiednie i szczegółowe środki zapewniające osobie, której dane dotyczą, poszanowanie jej godności, prawnie uzasadnionych interesów i praw podstawowych, **w szczególności pod względem** przejrzystości przetwarzania, **przekazywania danych osobowych** w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą oraz systemów monitorujących w miejscu pracy.

Sankcje finansowe

W zależności od kategorii naruszenia przepisów, RODO przewiduje kary finansowe w wysokości:

- do 10.000.000 EUR lub 2% całkowitego rocznego obrotu przedsiębiorstwa za rok poprzedni, lub
- do 20.000.000 EUR lub 4% całkowitego rocznego obrotu przedsiębiorstwa za rok poprzedni,

- przy czym w obu przypadkach zastosowanie znajdzie kara wyższa.

Zaangażowanie działów HR na poszczególnych etapach:

1. Zbieranie danych osobowych.
2. Informowanie podmiotów danych o zbieraniu danych.
3. Wybór kandydata – rekrutacja elektroniczna/profilowanie danych.
4. Zapewnienie dostępu do danych w trakcie zatrudnienia.
5. Zabezpieczenie danych.
6. Powierzenie przetwarzania danych podmiotom zewnętrznym.
7. Udostępnienie danych.
8. Powołanie ABI/IOD.
9. Zgłaszanie nieprawidłowości.
10. Budowanie świadomości wśród pracowników.

Zbieranie danych osobowych

Jakie dane osobowe mogą być zbierane?

• Problematyczny w praktyce art. Art. 22^1 k.p. – zbyt wąski katalog danych

Czy to katalog zamknięty?

• W teorii tak…

Jak jest w praktyce?

• Dopuszcza się przetwarzanie na innych, ogólnych podstawach.

INFOR | WIDEO AKADEMIA

Zbieranie danych osobowych

Musi być spełniony **co najmniej jeden** z poniższych warunków:

a. osoba, której dane dotyczą wyraziła **zgodę** na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

b. 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;

c. przetwarzanie jest niezbędne do wypełnienia **obowiązku prawnego** ciążącego na administratorze;

d. przetwarzanie jest niezbędne do **ochrony żywotnych interesów osoby**, której dane dotyczą, lub innej osoby fizycznej;

e. przetwarzanie jest niezbędne do **wykonania zadania realizowanego w interesie publicznym** lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

f. 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.

Zbieranie danych osobowych

Zgoda podmiotu danych - art. 4 pkt. 11 RODO

•„zgoda” osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych”.

•Jeśli przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą, administrator powinien być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na operację przetwarzania.

INFOR | WIDE AKADEMIA

Zbieranie danych osobowych

Sposób wyrażenia zgody:

a. oświadczenie woli,
b. zgoda konkludentna – wyrażana poprzez działanie dostatecznie ujawniające zamiar udzielenia zgody (okoliczności udzielenia zgody, zwyczaje w danej branży)

Zgoda musi być **jednoznaczna oraz świadoma**, co oznacza, m.in., że oświadczenie o wyrażeniu zgody przygotowane przez administratora powinno mieć zrozumiałą i łatwo dostępną formę, być sformułowane jasnym i prostym językiem i nie powinno zawierać nieuczciwych warunków (motyw nr 42).

Zbieranie danych osobowych

Zgoda w stosunku pracy?

Wyrażenia zgody nie należy uznawać za dobrowolne, jeżeli osoba, której dane dotyczą, nie ma rzeczywistego lub wolnego wyboru oraz nie może odmówić ani wycofać zgody bez niekorzystnych konsekwencji.

Aby zapewnić dobrowolność, zgoda nie powinna stanowić ważnej podstawy prawnej przetwarzania danych osobowych w szczególnej sytuacji, w której istnieje wyraźny brak równowagi między osobą, której dane dotyczą, a administratorem (motyw 43).

Czy „brak równowagi" odnosi się do stosunku pracy?

Zbieranie danych osobowych

Przesłanka usprawiedliwionego celu

Usprawiedliwiony cel występuje w przypadku:

- Przesyłania danych osobowych w ramach grupy przedsiębiorstw do wewnętrznych celów administracyjnych, co dotyczy też przetwarzania danych pracowników (!!!);
- Gdy dane są niezbędne do zapobiegania oszustwom;
- „Własnego" marketingu bezpośredniego;
- Gdy jest to niezbędne dla zapewnienia bezpieczeństwa sieci i informacji.

INFOR | WIDE AKADEMIA

Zbieranie danych osobowych

Podsumowanie - rola Działów HR na etapie zbierania danych:

- Kontrola jakie dane są zbierane i na jakiej podstawie (przepis prawa, usprawiedliwiony cel, zgoda).
- Czy kandydat/pracownik wyraził zgodę i czy mamy na to dowód.
- Czy klauzula zgody jest zrozumiała.
- W jakich warunkach zgoda jest wyrażona – dobrowolność.
- Czy zgoda nie została cofnięta.

Dostosowanie klauzul zgody i procesów pozyskiwania zgody

Informowanie podmiotów danych

O czym należy informować?

Zakres informacji, które mają być podane przy zbieraniu danych (art. 13 i 14 RODO) znacznie rozszerzony:

- Nie tylko oznaczenie administratora danych, ale także dane kontaktowe ABI/inspektora ochrony danych.
- Nie tylko cel przetwarzania, ale także podstawa prawna przetwarzania.
- Wskazanie uzasadnionych interesów jeżeli są one podstawą przetwarzania.
- Nie tylko pouczenie o prawie dostępu do danych, korekty i sprzeciwu, ale również o prawie do cofnięcia zgody, jeżeli jest ona podstawą przetwarzania oraz o prawie wniesienia skargi do organu nadzorczego.
- Informacja o zamiarze przekazania danych do państwa trzeciego oraz o gwarancjach odpowiedniego poziomu ochrony danych w tym państwie.
- O okresie przechowywania danych lub kryteriach jego ustalania (!).
- O profilowaniu.

Informowanie podmiotów danych

Rola Działu HR – weryfikacja czy:

- informujemy o wszystkim
- klauzule są jasne i zrozumiałe
- informacja jest przekazywana w terminie

Konieczność dostosowania klauzul informacyjnych!!!

Wybór kandydata / profilowanie

Co to jest profilowanie? (art. 4 pkt. 4 RODO)

„oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które 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”

Jak może być wykorzystane w procesie rekrutacji?

Profilowanie może być wykorzystywane jako automatyczne przetwarzanie aplikacji kandydata w elektronicznej rekrutacji. Niekiedy może wymagać na ostatnim etapie **weryfikacji przez człowieka** – rola Działu HR.

INFOR | WIDEO AKADEMIA

Dostęp do danych

Pod rządami **RODO poszerzenie prawa dostępu** do danych:

Przekazanie podmiotowi danych **na jego żądanie** określonych informacji, których zakres został rozszerzony analogicznie do katalogu informacji przekazywanych przy zbieraniu danych (art. 13 i 14 RODO)

Sposób realizacji prawa dostępu do danych (art. 15 ust.3 RODO)

- Dostarczenie przez Administratora osobie, której dane dotyczą, **jedną kopię** danych osobowych podlegających przetwarzaniu.
- Za wszelkie kolejne kopie administrator może pobrać **opłatę** w rozsądnej wysokości wynikającej z kosztów administracyjnych.
- Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji **udziela się powszechnie stosowaną drogą elektroniczną**.

Dostęp do danych

Rola Działu HR:

- Będzie często adresatem takiego zapytania;
- Identyfikacja jakie dane są przetwarzane;
- Przekazanie danych.

Stworzenie procedur odpowiedzi na zapytania.

Zabezpieczenie danych

Pracodawca jest obowiązany zastosować **środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych**. Przede wszystkim zobowiązany jest **zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym**, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, **uszkodzeniem lub zniszczeniem**.

Dotyczy to zarówno pracodawców przechowujących dane w **formie papierowej**, jak i w formie zbioru danych w **systemie informatycznym**.

INFOR | WIDEO AKADEMIA

Zabezpieczenie danych

Ustawodawca nie określił konkretnych technicznych środków zabezpieczenia. Pracodawca musi zastosować środki techniczne i organizacyjne adekwatne do zagrożeń („analiza ryzyka”)

Przy aktach papierowych np.:

- zamykane szafy na akta;
- szafy w osobnych odizolowanych pomieszczeniach;
- dostęp zarówno do pomieszczeń i szaf można zabezpieczyć odpowiednimi zamkami, również elektronicznymi, wymagającymi np. kodów dostępu, czy kart chipowych;
- polityka czystego biurka.

Zabezpieczenie danych

Rola Działu HR

- Dział HR może pomóc administratorowi danych zidentyfikować najbardziej adekwatne do zagrożeń możliwości zabezpieczenia danych.
- Dopilnowanie działania zabezpieczeń w praktyce (hasła, polityka czystego biurka).
- Udział przy nadawaniu upoważnień - dostęp do danych tylko dla osób upoważnionych – Dział HR na straży wykonania tego obowiązku!!!

Powierzenie przetwarzania danych

Pod rządami RODO:

Administrator ma obowiązek korzystania tylko z usług takich **podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków** technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

Umowa o powierzeniu przetwarzania danych – jej treść pod rządami RODO została istotnie zmodyfikowana.

Rola Działu HR:

- wybór dostawców usług płacowych,
- weryfikacja umów z nimi zawartych (czy są zawarte i jaka jest ich treść).

INFOR | WIDEO AKADEMIA

Udostępnianie danych

Udostępnianie danych osobowych można określić jako wszelkie działania umożliwiające innym, niż administrator, podmiotom zapoznanie się z nimi (*z wyłączeniem np.: osoby upoważnionej do przetwarzania danych; podmiotu, który przetwarza dane na podstawie umowy powierzenia).*

Należące do tej samej grupy kapitałowej spółki, są odrębnymi administratorami.

Nie należy bezrefleksyjnie przekazywać danych osobowych! Nawet do „spółki matki”!

Udostępnianie danych

Rolą Działu HR jest sprawdzenie:

- Czy administrator, który prosi nas o udostępnienie danych ma ku temu podstawę/w jakim celu prosi te dane?

  Usprawiedliwiony cel/ zgoda/ inna podstawa prawna?

- Czy wszystkie te dane, o które prosi nas inny administrator, są rzeczywiście potrzebne dla realizacji wskazanego celu?

  •Zakres pozyskiwanych danych musi być adekwatny i ograniczony do niezbędnego minimum dla realizacji wskazanego celu. Niekiedy wystarczy przekazania danych w formie spseudonimizowanej (pseudonimizacja polega na zakryciu lub zastąpieniu informacjami niezrozumiałymi dla odbiorcy, na przykład inicjały imion osób lub pierwsze litery nazw miast)

- Do jakiego kraju przekazujemy dane.

  •Dodatkowe wymogi w przypadku przekazania do państw trzecich.

ABI / IOD

Administrator Bezpieczeństwa Informacji – Inspektor Ochrony Danych Osobowych

Powołanie ABI jest uprawnieniem administratora danych. Powołanie IODO niekiedy będzie obowiązkowe.

IOD może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług.

Rola Działu HR

To dział HR zapewne **będzie rekrutować**, musi mieć zatem świadomość wymogów jakie wobec ABI/IODO stawiają przepisy.

Dział HR będzie też współtworzył **zakres obowiązków i budował strukturę organizacyjną.**

Zgłaszanie nieprawidłowości

Definicja **naruszenia danych osobowych** (art. 4 pkt. 12 RODO)

„oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych”

- Obowiązek powiadomienia organu nadzoru **w ciągu 72 godzin** od ich stwierdzenia !!!
- Obowiązek powiadomienia administratora przez podmiot przetwarzający.
- Obowiązek powiadomienia podmiotu danych osobowych.

Zgłaszanie nieprawidłowości

Rola Działu HR:

- informowanie administratora o dostrzeżonych naruszeniach,
- uświadamianie innym pracownikom konieczności zgłaszania naruszeń,
- pomoc Administratorowi w opracowaniu rozwiązań pozwalających uniknąć takich naruszeń w przyszłości.

Budowanie świadomości

Jak wskazano powyżej Rola działów HR w zakresie ochrony danych osobowych i prawidłowym ich przetwarzaniu jest kluczowa.

Działy HR powinny dbać także o budowanie świadomości
w zakresie ochrony danych osobowych:

- bieżące – zwracać uwagę pracownikom i współpracownikom na zauważone nieprawidłowości, np. pozostawianie dokumentów zawierających dane klientów/pracowników w miejscach do których mogą mieć dostęp osoby nieuprawnione;
- długoterminowe – zapewniać odpowiednie szkolenia dla siebie oraz swoich pracowników i współpracowników.

Budowanie świadomości

To, jak traktujemy dane osobowe pracowników, pokazuje jak traktujemy dane osobowe klientów.

Budowanie świadomości o ochronie danych osobowych wewnątrz organizacji przekłada się na budowanie wizerunku danego podmiotu na zewnątrz – wśród naszych klientów.

Ochrona danych osobowych jest istotnym elementem budowania wizerunku firmy.

INFOR | WIDEO AKADEMIA