INFORAKADEMIA

Ochrona danych osobowych pracowników – co się zmieni pod rządami RODO

Paulina Szymczak-Kamińska

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

INFORAKADEMIA

Zbieranie i przetwarzanie danych osobowych pracowników

INFORAKADEMIA

Czy katalog danych pracowników przetwarzanych przez pracodawcę zmieni się pod rządami RODO?

RODO w art. 88 daje państwom członkowskim możliwość zawarcia w swoich przepisach lub w porozumieniach zbiorowych bardziej szczegółowych przepisów mających zapewnić ochronę praw i wolności w przypadku przetwarzania danych osobowych pracowników w związku z zatrudnieniem, w szczególności do celów:

- rekrutacji,
- wykonania umowy o pracę, w tym wykonania obowiązków określonych przepisami lub porozumieniami zbiorowymi,
- zarządzania, planowania i organizacji pracy,
- równości i różnorodności w miejscu pracy,
- bezpieczeństwa i higieny pracy,
- ochrony własności pracodawcy lub klienta
- oraz do celów indywidualnego lub zbiorowego wykonywania praw i korzystania ze świadczeń związanych z zatrudnieniem,
- a także do celów zakończenia stosunku pracy.

INFORAKADEMIA

Czy katalog danych pracowników przetwarzanych przez pracodawcę zmieni się pod rządami RODO?– nowy projekt ustawy

Państwo polskie skorzystało z możliwości przyjęcia szczególnych regulacji na podstawie art. 88 RODO - Ministerstwo Cyfryzacji przygotowało projekt ustawy – przepisy wprowadzające ustawę o ochronie danych osobowych.

INFORAKADEMIA

Zmiany w Kodeksie pracy a RODO
Art. 22 [1] k.p.

§ 1. 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;
4.miejsce zamieszkania (adres do korespondencji);
5.wykształcenie;
6.przebieg dotychczasowego zatrudnienia.

§ 1. Pracodawca **żąda** od osoby ubiegającej się o zatrudnienie podania danych osobowych obejmujących:

1.imię (imiona) i nazwisko;
2.datę urodzenia;
3.dane kontaktowe wskazane przez taką osobę;
4.wykształcenie;
5.przebieg dotychczasowego zatrudnienia.

INFORAKADEMIA

Zmiany w Kodeksie pracy a RODO
Art. 22 [1] k.p.

§ 2. Pracodawca ma prawo żądać od pracownika podania **niezależnie od danych osobowych, o których mowa w § 1** także:

1.innych danych osobowych pracownika, a także imion i nazwisk oraz dat urodzenia dzieci pracownika, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy;
2.numeru PESEL pracownika nadanego przez Rządowe Centrum Informatyczne Powszechnego Elektronicznego Systemu Ewidencji Ludności (RCI PESEL).

§ 2. Pracodawca żąda od pracownika podania **dodatkowo** danych osobowych obejmujących:

1.adres zamieszkania;
2.numer PESEL**, a w przypadku jego braku – rodzaj i numer dokumentu potwierdzającego tożsamość**;
3.inne dane osobowe pracownika, a także dane osobowe dzieci pracownika i innych członków jego najbliższej rodziny, **jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy.**

INFORAKADEMIA

Zmiany w Kodeksie pracy a RODO
(…) po art. 22^1 dodaje się art. 22^2 - 22^5 w brzmieniu: Art. 22^2 KP

§ 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.

INFORAKADEMIA

Zmiany w Kodeksie pracy a RODO
(…) po art. 22^1 dodaje się art. 22^2 - 22^5 w brzmieniu: Art. 22^2 KP

*O tym, czy podanie określonych danych spełnia przesłankę **„bycia korzystnym”** dla kandydata lub pracownika, będą oceniały **obie** strony stosunku pracy. Natomiast **ostateczną** decyzję, czy podanie tych danych **rzeczywiście** leży w interesie pracownika, będzie podejmował **pracownik**, udzielając zgody na ich przewarzanie lub odmawiając jej udzielenia.*

*Ponadto wskazanie w przepisie, iż dane „za zgodą” można pobrać bezpośrednio od kandydata lub pracownika uniemożliwi pracodawcom stosowanie praktyki tzw. „**background screeningu**”, czyli pozyskiwania danych osobowych od osób trzecich (np. byłych pracodawców).*

INFORAKADEMIA

Dane o niekaralności obecnie

Pracodawca nie może żądać podania takich informacji. Jedynym wyjątkiem jest **istnienie przepisu prawa, który wyraźnie daje takie uprawnienie**. Przepisy ustawy o krajowym rejestrze karnym przewidują, że wyłącznie pracodawcy, którzy posiadają takie uprawnienie na mocy innych ustaw i tam **przewidziany jest wymóg niekaralności dla pracownika** mogą żądać takich informacji od kandydatów. Takimi przykładami będą: taksówkarze, strażnicy miejscy czy też nauczyciele.

INFORAKADEMIA

Dane o niekaralności pod rządami RODO

W RODO przewidziano **autonomiczną** regulację dotyczącą przetwarzania danych dotyczących **wyroków skazujących i naruszeń prawa.**
Przetwarzanie jest dopuszczalne:

- **wyłącznie** pod nadzorem władz publicznych lub,
- Jeżeli przetwarzanie jest **dozwolone** prawem UE lub **prawem państwa** członkowskiego, **pod warunkiem odpowiedniego** zabezpieczenia **praw** i **wolności** osób, których te dane dotyczą.

INFORAKADEMIA

Dane o niekaralności pod rządami RODO – projekt ustawy

12 kwietnia Sejm przyjął projekt ustawy o zasadach pozyskiwania informacji o niekaralności osób ubiegających się o zatrudnienie i osób zatrudnionych w podmiotach sektora finansowego. Tekst ustawy został teraz przekazany do prac Senatu.

Projekt ustawy przyznaje pracodawcom sektora finansowego uprawnienie do badania niekaralności osób zatrudnionych i osób ubiegających się o zatrudnienie w tych podmiotach na stanowiskach związanych z zarządzaniem mieniem tego podmiotu lub osób trzecich, dostępem do informacji prawnie chronionych lub stanowiskach związanych z podejmowaniem decyzji obarczonych wysokim ryzykiem utraty mienia tego podmiotu sektora finansowego lub osób trzecich lub wyrządzenia innej znacznej szkody temu podmiotowi sektora finansowego lub osobom trzecim.

W uchwalonej ustawie znajduje się zamknięty katalog przestępstw w zakresie których uprawnione będzie weryfikowanie kandydatów do pracy i osób zatrudnionych.

Niezłożenie oświadczenia bądź informacji z KRK lub udzielenie informacji potwierdzających skazanie prawomocnym wyrokiem za przestępstwo może stanowić przyczynę niezatrudnienia kandydata do pracy, a w przypadku osoby zatrudnionej może stanowić przyczynę rozwiązania stosunku pracy za wypowiedzeniem lub rozwiązania innej umowy bez względu na podstawę prawną świadczenia pracy.

INFORAKADEMIA

Inne niż Kodeks pracy podstawy prawne przetwarzania danych pracowników

Obecnie dane „zwykłe” mogą być przetwarzane w oparciu o jedną z podstaw wskazanych w art. 23 ust. 1 Ustawy:

a) zgodę osoby, której dane dotyczą;
b) niezbędność dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa;
c) jeżeli jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą;
d) jeżeli jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

INFORAKADEMIA

Katalog podstaw prawnych przetwarzania danych osobowych pod rządami RODO

Katalog podstaw prawnych przetwarzania danych został wskazany w art. 6 RODO.

Z punktu widzenia pracodawcy najważniejsze z nich to:

a) zgoda osoby, której dane dotyczą – podstawa ta została doprecyzowana w art. 7 RODO, o czym będzie mowa poniżej;
b) jeśli jest to 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) jeśli jest to niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
d) jeśli jest to niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przed 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.

Biorąc pod uwagę powyższy katalog, podstawy prawne przetwarzania danych w RODO będą w zasadzie takie same jak obecnie. Pojawi się jednak nowa konstrukcja prawna zgody oraz ogólne warunki jej wyrażenia. Doprecyzowana zostanie również przesłanka usprawiedliwionego celu, o czym będzie mowa poniżej.

Zgoda jako podstawa przetwarzania danych w stosunku pracy - obecnie

Co do zasady zgoda jest dopuszczalna ale MUSI BYĆ DOBROWOLNA.
Dobrowolność zgody była kwestionowana przez GIODO i przez NSA.

Z drugiej jednak strony, nie można z góry zakładać, że zgoda pracownika wyrażona w relacji z pracodawcą nie jest dobrowolna. Wiele przepisów kodeksu pracy wymaga zgody pracownika – przykładowo zgoda na potrącenie należności z wynagrodzenia pracownika (art. 91 k.p.).

Można wobec tego posłużyć się zgodą kandydata/pracownika, ale tylko wówczas, jeśli odnosi się ona do przypadku, w którym pracownik ma całkowitą swobodę jej udzielenia i może odmówić udzielenia takiej zgody bez żadnych negatywnych konsekwencji (tak m.in. wyrok WSA w Warszawie z 20 czerwca 2011 r., sygn. akt SA/Wa 719/11).

INFORAKADEMIA

Zgoda pracownika w RODO

W motywie 155 znajduje się wzmianka o tym, że państwa członkowskiego mogą wprowadzić szczegółowe przepisy dotyczące przetwarzania danych osobowych pracowników w kontekście zatrudnienia, w szczególności warunki, na których dane osobowe można przetwarzać za zgodą pracownika.

RODO przewiduje zatem co do zasady możliwość przetwarzania danych na podstawie zgody pracownika. Potwierdza to także fakt, że w RODO nie znalazła się ostatecznie wzmianka o tym, że brak równowagi zachodzi w szczególności w stosunku pracy, która pojawiała się w projektach RODO.

INFORAKADEMIA

Zgoda pracownika w RODO

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".

Wykazanie uzyskania zgody podmiotu danych - art. 7 ust. 1 RODO
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.

W zrozumiałej i łatwo **dostępnej formie, jasnym i prostym językiem**.

Podmiot danych ma **prawo w dowolnym momencie wycofać** udzieloną wcześniej zgodę na przetwarzanie danych. Wycofanie zgody **nie wpływa na dotychczasową zgodność z prawem przetwarzania** prowadzonego na podstawie zgody przed jej wycofaniem (*skutek ex nunc*). Wycofanie zgody musi być równie **łatwe**, jak jej wyrażenie – niedopuszczalne jest stawianie sztucznych nieuzasadnionych barier dla odwołania zgody.

INFORAKADEMIA

Zgoda wyrażona przed rozpoczęciem stosowania RODO

Motyw 171 RODO: *Jeżeli przetwarzanie ma za podstawę zgodę w myśl dyrektywy 95/46/WE, osoba, której dane dotyczą, nie musi ponownie wyrażać zgody, jeżeli pierwotny sposób jej wyrażenia odpowiada warunkom niniejszego rozporządzenia; dzięki temu administrator może kontynuować przetwarzanie po dacie rozpoczęcia stosowania niniejszego rozporządzenia.*

Zasadniczo nie zmieniły się warunki pozwalające uznać dane oświadczenie za prawnie wiążącą zgodę (jak wspomniany wymóg dobrowolności). Co więcej zmianie ulegnie charakter prawny zgody w porównaniu z obecnym stanem prawnym. Zgodę wyraźną w rozumieniu ustawy o ochronie danych osobowych zastąpi zgoda jednoznaczna.

Wobec tego „poluzowania" charakteru prawnego zgód, wydaje się, że większość otrzymanych dotychczas zgód zachowa ważność także pod rządami ogólnego rozporządzenia. Pod warunkiem, że poinformowano osobę, której dane dotyczą o możliwości wycofania zgody w dowolnym momencie, a wycofanie zgody jest równie łatwe jak jej wyrażenie.

INFORAKADEMIA

Informowanie podmiotów danych (pracowników) o zbieraniu danych

INFORAKADEMIA

Jak informować podmioty danych?

Administrator powinien podjąć wszelkie środki aby obowiązek informacyjny spełnić w **zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie**, a także przy użyciu **jasnego i prostego języka.**

Obowiązek poinformowania powinien zostać spełniony na **piśmie lub w inny sposób np. elektronicznie**.

W razie żądania osoby, której dane dotyczą, informacji można udzielić **ustnie**, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.

Co do zasady za czynność informowania **nie można pobierać opłat**!
Wyjątek: jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter – w takich sytuacjach administrator może pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań albo odmówić udzielenia informacji.
Uwaga: Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze.

INFORAKADEMIA

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.

INFORAKADEMIA

Informowanie podmiotów danych

W przypadku pozyskiwania danych **nie od osoby, której dotyczą:**

o **kategoriach** pozyskanych danych

o **źródle** pochodzenia danych (w tym czy pochodzą ze źródeł publicznie dostępnych).

ALE zmienił się **termin** przekazania tych danych:

Poprzednio: „bezpośrednio po utrwaleniu zebranych danych”

Obecnie: „w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca - mając na uwadze konkretne okoliczności przetwarzania danych osobowych”

INFORAKADEMIA

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!!!!

INFORAKADEMIA

Zapewnienie dostępu do danych w trakcie zatrudnienia

INFORAKADEMIA

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).

Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora: 1) **potwierdzenia**, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, 2) jest uprawniona do uzyskania **dostępu** do nich oraz uzyskania **informacji** takich jak z art. 13 i 14 RODO (cele przetwarzania; kategorie odnośnych danych osobowych; informacje o odbiorcach lub kategoriach odbiorców, okres przechowywania danych osobowych, itp.)

INFORAKADEMIA

Dostęp do danych

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**.

INFORAKADEMIA

Dostęp do danych

Termin - bez zbędnej zwłoki – a w każdym razie w terminie **miesiąca** od otrzymania żądania.

W razie potrzeby termin ten można **przedłużyć o kolejne dwa** miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań.

W terminie miesiąca od otrzymania żądania administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia.

Jeżeli administrator **nie podejmuje działań** w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

INFORAKADEMIA

Zabezpieczenie danych pracowników

INFORAKADEMIA

Zabezpieczanie 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**.

INFORAKADEMIA

Zabezpieczanie danych

Zabezpieczenie danych w formie papierowej

Obowiązek przechowywania **akt osobowych** pracowników przez okres 50 lat od dnia zakończenia stosunku pracy, a w przypadku dokumentacji płacowej - 50 lat licząc od dnia jej wytworzenia.

Ustawodawca nie określił konkretnych technicznych środków zabezpieczenia akt osobowych przechowywanych w formie papierowej. Pracodawca musi zastosować takie środki techniczne i organizacyjne, aby zabezpieczyć akta, może więc korzystać z wszelkich rozwiązań zapewniających wykonanie tego zadania, 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.**

INFORAKADEMIA

Zabezpieczanie danych

Zabezpieczanie danych w systemie informatycznym

Obecnie - Rozporządzenie ministra spraw wewnętrznych
i administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych - „check list”.

Pod rządami RODO - „analiza ryzyka” - zabezpieczenia mają być adekwatne do zagrożeń.

Rola Działu IT

INFORAKADEMIA

Zabezpieczanie 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!!!

Forma upoważnienia do przetwarzania danych osobowych:
pisemna (nie jest wymagana, choć dogodna ze względów dowodowych);
służbowy e-mail archiwizowany w celach dowodowych.

Treść: data nadania i ustania oraz zakres upoważnienia.

INFORAKADEMIA

Powierzenie przetwarzania danych pracowników podmiotom zewnętrznym

INFORAKADEMIA

Powierzenie przetwarzania

Forma umowy o powierzeniu przetwarzania danych

forma pisemna

Treść umowy o powierzeniu przetwarzania danych

szczegółowe określenie zakresu i celu przetwarzania powierzonych danych, przykładowo:

zakres – dane osobowe pracowników spółki

cel – obsługa płacowa

INFORAKADEMIA

Powierzenie przetwarzania

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).

INFORAKADEMIA

Udostępnienie danych pracowników

INFORAKADEMIA

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”!

INFORAKADEMIA

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.

INFORAKADEMIA

Udostępnianie danych

Przekazywanie danych osobowych do państw trzecich:

1. Przekazywanie danych do państw **w ramach Unii Europejskiej i EOG:**

   na takich samych zasadach jak na terytorium Polski.

2. Przekazywanie danych **do państw trzecich -** dodatkowe wymogi:

   państwa te zapewniają adekwatny poziom ochrony;

   Komisja Europejska może stwierdzić, że państwo trzecie zapewnia odpowiedni stopień ochrony danych osobowych na podstawie swojego prawa krajowego lub zobowiązań międzynarodowych – wówczas przekazywanie danych do tego państwa nie będzie wiązało się z koniecznością spełnienia dodatkowych obowiązków (Privacy Shield, Szwajcaria, Kanada, Argentyna);

   w razie braku stwierdzenia odpowiedniego stopnia ochrony administrator lub podmiot przetwarzający mogą skorzystać z:

   - wiążących reguł korporacyjnych (BCR – Binding Corporate Rules);
   - **standardowych klauzul ochrony danych osobowych przyjętych przez Komisję**;
   - klauzul umownych przyjętych lub dopuszczonych przez organ nadzorczy (GIODO).

INFORAKADEMIA

Powołanie ABI/IODO

INFORAKADEMIA

ABI

Powołanie ABI było uprawnieniem administratora danych.

ABI – osoby pełniące funkcję w dniu 24 maja 2018 mają pełnić funkcję inspektora ochrony danych do 1 września 2018 – w tym czasie obowiązek administratora o wyznaczeniu IOD albo o tym że ABI nie pełni funkcji IOD

INFORAKADEMIA

IODO

IODO czyli **inspektor ochrony danych osobowych**.

- każdy podmiot powinien potrafić wykazać, iż przeprowadził stosowne analizy w celu ustalenia obowiązku bądź braku obowiązku wyznaczenia IOD

- obowiązkowe wyznaczenie:

  1. główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę;

  2. główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych albo danych osobowych dotyczących wyroków skazujących i naruszeń prawa

  3. organy i podmioty publiczne

INFORAKADEMIA

IODO

- kwalifikacje zawodowe
- nie musi być pracownikiem administratora – możliwy outsourcing
- administrator – obowiązek opublikowania danych kontaktowych IOD i zawiadomienia organu nadzorczego
- administrator ma obowiązek wspierać IOD w wypełnianiu przez niego zadań, co sprowadza się do:
  1) zapewnienia IOD zasobów niezbędnych do wykonania tych zadań,
  2)zapewnienia dostępu do danych osobowych i operacji przetwarzania,
  3) zapewnienia zasobów niezbędnych do utrzymania wiedzy fachowej IOD, np. poprzez udział w kursach/szkoleniach

INFORAKADEMIA

IODO

IODO powinien być właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych (Art. 38 ust. 1 RODO)

Administrator ma zapewnić IODO zasoby niezbędne do wykonywania zadań (Art. 38 ust. 2 RODO) i utrzymania jego wiedzy fachowej

IODO nie może otrzymywać instrukcji dot. wykonywania swoich zadań i podlega bezpośrednio najwyższemu kierownictwu
(Art. 38 ust. 3 RODO)

Wykonywanie przez IODO innych zadań nie może powodować konfliktu interesów
(Art. 38 ust. 6 RODO)

INFORAKADEMIA

Zgłaszanie nieprawidłowości

INFORAKADEMIA

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.

INFORAKADEMIA

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.

INFORAKADEMIA

Dziękuję za uwagę.

Paulina Szymczak-Kamińska

INFORAKADEMIA