ZMIANY W PRAWIE UE
W ZAKRESIE OCHRONY DANYCH OSOBOWYCH

NOWE ROZWIĄZANIA OCHRONY DANYCH WPROWADZONE PRZEZ ROZPORZĄDZENIE Z 27 KWIETNIA 2016 - JAK SIĘ PRZYGOTOWAĆ?

OMÓWIENIE KLUCZOWYCH ZMIAN DLA FIRM I JEDNOSTEK ORGANIZACYJNYCH

Autor: Karol Cieniak
Dyrektor Działu Prawnego RDBO

RBDO
REJESTRACJA I BEZPIECZEŃSTWO DANYCH OSOBOWYCH

Spis treści

1. **Wstęp**

2. **Nowe rozwiązania wprowadzone przez rozporządzenie**

a) Terytorialny zakres zastosowania
b) Rozróżnienie skali działalności
c) Obowiązek „rejestrowania czynności przetwarzania"
d) Obowiązek zgłoszenia naruszenia ochrony danych osobowych do organu nadzorczego
e) Ogólne obowiązki administratora danych osobowych
f) Zatwierdzone kodeksy postępowania
g) Proces dobrowolnej certyfikacji
h) Wyznaczenie wewnętrznego inspektora ochrony danych
i) Uregulowanie wieku pozwalającego na wyrażenie zgody na przetwarzanie danych w celu „usług społeczeństwa informacyjnego"

3. Nowe definicje

a) Profilowanie
b) Pseudonimizacja
c) Dane dotyczące zdrowia
d) Dane genetyczne
e) Dane biometryczne
f) Pojęcie jednostki organizacyjnej
g) Definicja zgody

4. Sankcje

a) Nie tylko kary pieniężne
b) Kryteria decydowania o zastosowaniu kar pieniężnych lub innych środków.
c) Wysokość kar pieniężnych

5. Możliwość ustanowienia przez państwa członkowskie przepisów szczególnych w określonych przypadkach

a) Przetwarzanie danych przez kościoły oraz związki lub wspólnoty wyznaniowe
b) Kontrolowanie przetwarzania danych osobowych objętych tajemnicą zawodową
c) Przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych, historycznych lub do celów statystycznych
d) Przetwarzanie danych osobowych w kontekście zatrudnienia
e) Przetwarzanie krajowego numeru identyfikacyjnego
f) Przetwarzanie danych zawartych w dokumentach urzędowych, które posiada organ, podmiot publiczny lub podmiot prywatny w celu wykonania zadania realizowanego w interesie publicznym
g) Przetwarzanie danych osobowych w związku wolnością wypowiedzi i informacji

Najważniejsze zmiany

1. **Wprowadzenie obowiązku prowadzenia „rejestru czynności przetwarzania" w określonych w rozporządzeniu przypadkach.**

2. **Wprowadzenia możliwości ustanawiania „kodeksów postępowania", określających sposoby realizacji procedur zabezpieczenia danych w określonych kategoriach podmiotów.**

3. **Wprowadzenie możliwości przyjęcia „mechanizmów certyfikujących" odnoszących się do sposobu określenia procedur przetwarzania danych w konkretnych podmiotach.**

4. **Wprowadzenie dodatkowych kryteriów warunkujących obowiązek ustanowienia wewnętrznego „inspektora ochrony danych" (odpowiednika ABI).**

5. **Obowiązek zgłaszania naruszenia ochrony danych do organu nadzorczego w ciągu 72 godzin.**

6. **Obowiązek dokonywania w określonych sytuacjach „oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych".**

7. **Wprowadzenie nowych kar pieniężnych nakładanych w trybie administracyjnym za naruszenia określonych przepisów ochrony danych osobowych sformułowanych w ogólnym rozporządzeniu o ochronie danych nawet do 20 milionów euro.**

8. **Określenie sfer, w których państwa członkowskie we własnym zakresie ustalą szczególne regulacje odnoszące się do ochrony danych w ramach prawa danego państwa członkowskiego.**

9. **Wprowadzenie określenie definicji takich czynności jak „profilowanie", „pseudonimizacja".**

10. **Zmiana sposobu (formy) uregulowania europejskiego prawa ochronnych danych z dyrektywy na rozporządzenie (które w przeciwieństwie do dyrektywy zawsze może być bezpośrednio stosowane w pełnym zakresie).**

1.Wstęp

Przegłosowane w Parlamencie Europejskim dnia 14 kwietnia 2016 roku „ogólne rozporządzenie o ochronie danych" z jednej strony wprowadza nowe zasady związane z przetwarzaniem danych osobowych w państwach członkowskich Unii Europejskiej, z drugiej strony utrwala i powtarza wiele przepisów istniejących już wcześniej, zwłaszcza na gruncie dyrektywy 95/46/WE. Już na początku preambuły, w ustępie 4 zostaje podkreślone, że „prawo do ochrony danych osobowych nie jest prawem bezwzględnym; należy je postrzegać w kontekście jego funkcji społecznej i wyważyć względem innych praw podstawowych w myśl zasady proporcjonalności." Należy zauważyć, że takie podejście do kwestii związanych z ochroną danych osobowych nie jest żadną zmianą w stosunku do poprzednio obowiązujących przepisów, co wielokrotnie dostrzegane było zarówno w orzecznictwie Europejskiego Trybunału Sprawiedliwości (wyrok sprawach połączonych C-9 2/09 i C-9 3/09 z dnia 9 listopada 2010 roku), jak polskich sądów administracyjnych.

W tym przypadku (a także w wielu innych kwestiach, co zostanie opisane w dalszej części) rozporządzenie powtarza znaczną część zasad, które zostały wprowadzone do unijnego dorobku prawnego w poprzednich latach. W dalszej części preambuły zostaje położony nacisk na „zdecydowane egzekwowanie stabilnych i spójnych ram ochrony danych w Unii", co uzasadnione jest zmianami społeczno-gospodarczymi, głównie rozwojem nowych technologii związanym ze skalą i znaczeniem zbierania i wymiany danych osobowych –fragment o "zdecydowanym egzekwowaniu" można odnieść to jednej z „nowości" wprowadzanych rozporządzeniem, czyli kar finansowych za naruszenie zasad ochrony danych osobowych (o czym w dalszej części).

Wiele postanowień zawartych w liczącym 88 stron (łącznie z preambułą) dokumencie zostało wręcz bezpośrednio zaczerpniętych ze wspomnianej dyrektywy – np. określenie zakresu obowiązywania:

- *Niniejsza dyrektywa stosuje się do przetwarzania danych osobowych w całości lub w części w sposób zautomatyzowany oraz innego przetwarzania danych osobowych, stanowiących część zbioru danych lub mających stanowić część zbioru danych* (art. 3 ust. 1 dyrektywy).

- *Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w sposób w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowychdanych stanowiących część zbioru danych lub mających stanowić część zbioru danych* (art. 2 ust. 1 rozporządzenia).

Należy podkreślić, że doniosłe znaczenie ma nie tylko wprowadzenie przez rozporządzenie całkowicie nowych, nie znanych do tej pory pojęć (o czym w dalszej części), ale istotny jest już sam fakt, nowej formy unijnego aktu prawnego odnoszącego się do spraw związanych z ochroną danych osobowych.

Rozporządzenie różni się od dyrektywy tym, że jest bezpośrednio stosowane w pełnym zakresie, natomiast sama dyrektywa co do zasady jest jedynie zobowiązaniem poszczególnego państwa członkowskiego do uregulowania przedmiotowej materii w prawie wewnętrznym tak, by zachowana była zgodność z dyrektywą - co ma takie znaczenie, że podmiot który np. poniósł szkodę w powodu braku prawidłowej transpozycji dyrektywy do prawa krajowego może dochodzić od państwa członkowskiego odszkodowania.

Dyrektywa więc, jako akt prawa unijnego, charakteryzuje się „bezpośrednim skutkiem wertykalnym" (wiąże bezpośrednio państwa członkowskie, organy publiczne – ale nie podmioty prywatne), natomiast **rozporządzenie charakteryzuje się „bezpośrednim skutkiem horyzontalnym", co oznacza, że jest skuteczne tak, jakby było ustawą lub innym aktem prawa krajowego bezpośrednio stosowanym.**

Nie należy się jednak spodziewać, by jedno unijne rozporządzenie całkowicie zastąpiło krajowe akty prawa wewnętrznego takie jak np. polska ustawa o ochronie danych osobowych, ponieważ pomimo możliwości bezpośredniego jego stosowania, rozporządzenie pozostawia wiele spraw które można by określić jako „szczegółowe" do wewnętrznej regulacji poszczególnym państwom członkowskim. Otwarte pozostaje pytanie jaką formę przyjmie uregulowanie przetwarzaniadanych osobowych na poziomie prawa polskiego – czy ustawa o ochronie danych z 1997 zostanie jedynie znowelizowana, czy też zostanie zastąpiona zupełnie nowym aktem prawnym.

Niewątpliwym skutkiem rozporządzenia będzie większe ujednolicenie oraz zharmonizowanie wewnętrznych porządków prawnych państw członkowskich – z uwagi jednak na obszary pozostawione państwom członkowskim do wewnętrznej regulacji należy się spodziewać, że to ujednolicenie nastąpi jedynie do pewnego stopnia.

Zapraszam do lektury i dyskusji,
Karol Cieniak
faq@rbdo.pl

Spełnij obowiązki ochrony danych wybierając zestaw dokumentacji ze wsparciem prawnym za 99 zł netto + 23% VAT lub wersję rozszerzoną Dokumentacji z Instrukcją rejestracji zbiorów do GIODO i wsparciem prawnym w tym zakresie za 199 zł netto + 23%

W cenie aplikacja do zarządzania systemem ochrony danych osobowych oraz materiały szkoleniowe!

Zapraszamy do zapoznania się z ofertą na stronach sklepu RBDO >>

2. Nowe rozwiązania wprowadzone przez rozporządzenie

a) Terytorialny zakres zastosowania.

Doprecyzowany został określony w art. 3 rozporządzenia terytorialny zakres zastosowania – gdzie jako bardzo szerokie kryterium określono działalność prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego dane w Unii – ale niezależnie od tego, czy samo przetwarzanie odbywa się w Unii. Podstawowym zatem kryterium kwalifikującym dany podmiot pod unijne prawo ochrony danych jest wykonywanie działalności na terenie jakiegokolwiek państwa członkowskiego, chociażby samo przetwarzanie miało miejsce już poza UE.

Art. 3 ust. 2 rozporządzenia precyzuje, że wystarczy by sama czynność przetwarzania była choćby związana z „oferowaniem towarów lub usług" osobom przebywającym na terenie Unii lub monitorowaniem zachowania osób przebywających na terenie Unii, by przepisy rozporządzenia miały zastosowanie do podmiotu prowadzącego taką działalność.

b) Rozróżnienie skali działalności

Za właściwy kierunek uznać należy zawarte w ustępie 13 preambuły rozróżnienie na kategorię mikroprzedsiębiorstw (a także małych i średnich) jako podmiotów zatrudniających mniej niż 250 pracowników, co do których powinny znaleźć zastosowanie mniej rygorystyczne wymogi, w tym przypadku dotyczące „rejestrowania czynności przetwarzania".

Dodać należy, że brak rozróżnienia pod względem skali prowadzonej działalności był jedną z największych wad dotychczasowego stanu prawnego, wystarczy zwrócić uwagę na fakt, że w rozumieniu polskiej ustawy bez względu na to, czy administrator przetwarza dane np. miliona klientów, czy stu klientów – jest on takim samym administratorem danych, który musi spełnić dokładnie te same wymagania od strony formalnej (pomijając przepisy regulujące specyficzne branże), w nowym unijnym rozporządzeniu co prawda ten problem nie został całkowicie rozwiązany, ale już samo dostrzeżenie problemu różnic w skali działalności należy uznać za krok w dobrym kierunku.

Sam „próg" zatrudnienia 250 pracowników ściśle jest związany z określonym w art. 30 rozporządzenia obowiązkiem „rejestrowania czynności przetwarzania", o czym poniżej. Otwarte pozostaje pytanie, czy stworzone przez rozporządzenie możliwości przyjęcia odrębnych „kodeksów postępowania" stworzonych w myśl art. 40 rozporządzenia np. na potrzeby specyficznej grupy drobnych przedsiębiorców działających w określonej branży wpłyną na ułatwienie wykonywania poszczególnych obowiązków wynikających z rozporządzenia – właśnie w kontekście skali prowadzonej działalności. By to stwierdzić, należy jednak poczekać na praktykę zatwierdzania przez organy nadzorujące konkretnych kodeksów postępowania.

Pewien problem interpretacyjny może też sprawiać zawarte między innymi w art. 37 kryterium „przetwarzania danych na dużą skalę", czego niestety nie doprecyzowano w rozporządzeniu, a stanowi jedno z kryteriów przesądzających o zaistnieniu obowiązku wyznaczenia inspektora ochrony danych, lub braku takiego obowiązku.

c) Obowiązek „rejestrowania czynności przetwarzania"

Art. 30 rozporządzenia wprowadza obowiązek prowadzenia przez administratora danych „rejestru czynności przetwarzania", który zawiera:

- *imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych*
- *cele 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 w organizacjach międzynarodowych;*
- *gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;*
- *jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;*
- *jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust.1 rozporządzenia (między innymi stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 lub zatwierdzonego mechanizmu certyfikacji)*

Kto ma obowiązek prowadzenia „rejestru czynności przetwarzania" ?

- **Przedsiębiorca lub podmiot zatrudniający powyżej 250 osób**
- **Przedsiębiorca lub podmiot zatrudniający mniej niż 250 osób, jeżeli**

- przetwarzanie, którego dokonuje, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą

- przetwarzanie nie ma charakteru sporadycznego

- obejmuje szczególne kategorie danych osobowych, o których mowa w art. 9 ust 1 rozporządzenia (pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne, a także dane dotyczących zdrowia, seksualności lub orientacji seksualnej). Oraz dane, o których mowa w art. 10 rozporządzenia (dane o naruszeniach prawa i wyrokach skazujących)

W praktyce może się okazać problematyczne, w jaki sposób należy interpretować sformułowanie o „sporadycznym charakterze" przetwarzania. Czy np. w przypadku sprzedaży internetowej do niezarejestrowanych kupujących będzie można jeszcze mówić o „sporadyczności", ale już w przypadku częstej praktyki polegającej na umożliwieniu klientom zakładania własnych kont, profili na serwisie sprzedażowym będzie to wykluczone?

d) Obowiązek zgłoszenia naruszenia ochrony danych osobowych do organu nadzorczego

Art. 33 ust. 1 rozporządzenia nakłada na administratora obowiązek niezwłocznego zgłoszenia do organu nadzorczego (w Polsce GIODO) naruszenia ochrony danych osobowych. Takie zgłoszenie administrator musi wykonać niezwłocznie, ale nie później niż w 72 godziny po stwierdzeniu naruszenia (a gdy a dministrator przekroczy ten termin, musi do zgłoszenia dołączyć wyjaśnienie przyczyn o późnienia).

Zgłoszenia nie należy dokonywać, jeżeli jest „mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych" - a zatem to na administratorze będzie ciążył ciężar oceny wraz z odpowiedzialnością z tym związaną (ocena prawdopodobieństwa ryzyka naruszenia praw lub wolności). Należy także pamiętać, że administrator jest zobowiązany do dokumentowania wszelkich naruszeń ochrony danych osobowych w ramach swojej dokumentacji wewnętrznej (niezależnie od tego czy dane naruszenia podlegało zgłoszeniu, czy nie). Jeżeli ryzyko naruszenia praw i wolności danej osoby jest wysokie, administrator musi poinformować także tą osobę, chyba że zachodzą wyjątki przewidziane w art. 34 ust. 3 rozporządzenia.

e) Ogólne obowiązki administratora danych osobowych

Art. 35 rozporządzenia wprowadza obowiązek dokonywania „oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych" w sytuacjach, gdy dany rodzaj przetwarzania ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. W praktyce natomiast należy spodziewać się podania do publicznej wiadomości przez GIODO (w związku z ustępami 4 oraz 5 wspomnianego artykułu) wykazów rodzajów operacji przetwarzania, które pod taki obowiązek będą podlegały, oraz takich, których przetwarzanie z takimi obowiązkami nie będzie się wiązało.

Efektem oceny, o której mówi wyżej wymieniony przepis może być skierowanie przez administratora wniosku o konsultacje, co do którego GIODO będzie miał obowiązek ustosunkować się w terminie n ie dłuższym niż 8 tygodni (z możliwością przedłużenia tego terminu maksymalnie o dodatkowe 6 tygodni).

Art. 24 rozporządzenia nakłada na administratora danych obowiązek wdrożenia „odpowiednich środków technicznych i organizacyjnych" - by przetwarzanie odbywało się zgodnie z rozporządzeniem i aby móc to wykazać. Dalej rozporządzenie wskazuje, że o ile jest to „proporcjonalne" jako wyżej wymienione środki należy rozumieć „przyjęcie odpowiednich polityk ochrony danych". Natomiast jako rozwiązanie związane z minimalizacją potencjalnego ryzyka polegającego na tym, że w danym przypadku środki przyjęte przez danego administratora mogły by zostać uznane za niewystarczające, w art. 24 ust. 3 przewiduje możliwość stosowania:

- zatwierdzonych kodeksów postępowania, o których mowa w art. 40 rozporządzenia lub
- zatwierdzonego mechanizmu certyfikacji, o którym mowa w 42 rozporządzenia

POLECAMY! JAK SPEŁNIĆ OBOWIĄZKI OCHRONY D ANYCH?

SPRAWDŹ CZY POSIADASZ OBOWIĄZEK REJESTRACJI ZBIORU DO GIODO – JEŚLI POSIADASZ CHOĆ 1 Z PONIŻSZYCH KATEGORII DANYCH:

- *zbiory danych Klientów (zawierające dowolne dane teleadresowe)*
- *dane korespondencyjne Klientów*
- *elektroniczne rejestry korespondencji (szkół, firm, jednostek organizacyjnych)*
- *bazy Newsletter*
- *bazy konkursowe*
- *rejestry wysyłkowe towarów*
- *rejestry reklamacji*
- *beneficjenci działań stowarzyszenia/klubu*
- *zbiory danych darczyńców*
- *rejestry uczniów, którzy wypełniają obowiązek szkolny poza daną szkołą*
- *uczestnicy konkursów międzyszkolnych*
- *zbiór danych osobowych czytelników czytelni*
- *listy akcjonariuszy (jeśli są tam osoby fizyczne)*
- *księgi gości, księgi meldunkowe*
- *rezerwacje imienne usług*
- *wszelkie inne dane osobowe, które nie podlegają zwolnieniu*

Polecanym rozwiązaniem regulującym wszystkie elementy przetwarzania danych podlagających rejestracji do GIODO jest wdrożenie **dokumentacji przetwarzania danych osobowych dla firm z Instrukcją zgłoszenia do GIODO – w cenie 199 zł netto + 23% VAT** wraz z pełnym wsparciem prawnym ekspertów RBDO w razie wątpliwości.

Zamówienie można złożyć na stronie sklepu **http://rbdo.pl/sklep/** lub przesyłając dane do Faktury Pro Forma na: **biuro@rbdo.pl**

RBDO.PL - Rejestracja i Bezpieczeństwo Danych Osobowych
ul. Kopalniana 22a/7 | 01-321 Warszawa
NIP: 522-302-50-86 | KRS: 0000549436
Tel.: +48 22 487 86 70 | Kom.: +48 664 484 218
biuro@rbdo.pl www.rbdo.pl

f) Zatwierdzone kodeksy postępowania

Z uwagi na specyfikę różnych sektorów działalności, często charakteryzujących się wyjątkowymi, właściwymi dla siebie zasadami postępowania, ale także uwzględniając szczególne potrzeby mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw, rozporządzenie przewiduje w art. 40 możliwość tworzenia „kodeksów postępowania".

Kodeksy postępowania rozporządzenie dzieli na dwie kategorie:

- zatwierdzone kodeksy postępowania w trybie art. 40 ust. 5 rozporządzenia (zatwierdzenia będzie dokonywał organ nadzorczy, a więc w Polsce GIODO, po przedłożeniu projektu kodeksu), zatwierdzony kodeks postępowania będzie przez GIODO rejestrowany i publikowany

- powszechnie obowiązujące kodeksy postępowania zgodnie z art. 40 u st. 9 rozporządzenia to takie kodeksy postępowania, które zostały w drodze aktu wykonawczego Komisji Europejskiej uznane za powszechnie obowiązujące w całej Unii – może to mieć miejsce jeżeli np. GIODO, w związku ze stwierdzeniem, że kodeks dotyczy postępowania w więcej niż jednym państwie członkowskim przekaże go przed zatwierdzeniem do Europejskiej Rady Ochrony Danych, która to rada następnie (w przypadku wydania pozytywnej opinii) przekaże go do Komisji Europejskiej

Co ciekawe, monitorowaniem przestrzegania zatwierdzonych kodeksów postępowania będzie mógł się zajmować nie tylko GIODO, ale także podmiot, który został przez GIODO akredytowany – taki podmiot posiadający akredytację będzie mógł zawiesić lub wykluczyć danego administratora lub podmiot przetwarzający z grona podmiotów stosujących kodeks, przy czym będzie jedynie musiał poinformować o tym GIODO, jako organ nadzorczy.

g) Proces dobrowolnej certyfikacji

Alternatywną do przyjmowania zatwierdzonych kodeksów postępowania przyjęcie dobrowolnego zatwierdzonego mechanizmu certyfikacji oraz jakości.

Certyfikacji dokonuje albo podmiot akredytowany (przez GIODO krajową jednostkę akredytującą), albo GIODO jako organ nadzorczy podstawie ustalonych kryteriów (a jeżeli te kryteria są zatwierdzone Europejską Radę Ochrony Danych, może to skutkować „europejskim jakości ochrony danych" jako efektem „wspólnej certyfikacji").

Administrator (lub podmiot przetwarzający) w celu uzyskania certyfikacji zobowiązany jest udzielić podmiotowi doko nującemu certyfikacji wszelkich informacji wszelkiego dostępu do swoich czynności przetwarzania, do których dostęp jest niezbędny do przeprowadzenia procedury certyfikacji.

Certyfikacji można dokonać na maksymalny okres 3 lat, po nastąpić jej przedłużenie lub cofnięcie.

Akredytacja podmiotów certyfikujących:

Warunki uzyskania akredytacji do dokonywania certyfikacji rozporządzenie w a rt. 43 ust. 2 określa jak:

- wykazały właściwemu organowi nadzorczemu swojej niezależność i wiedzy fachowej w dziedzinie podlegającej certyfikacji;
- zobowiązanie się do przestrzegania właściwych kryteriów mechanizmu certyfikacji, zatwierdzonego przez organ nadzorczy

- dysponowanie procedurami wydawania, okresowego przeglądu i cofania certyfikacji, znaków jakości i oznaczeń w dziedzinie ochrony danych;

- dysponowanie procedurami i strukturami, które pozwalają rozpatrywać skarg i na naruszenie warunków certyfikacji przez administratora lub podmiot przetwarzający lub na sposób wdrożenia lub wdrażania certyfikacji przez administratora lub podmiot przetwarzający, oraz które zapewniają przejrzystość tych procedur i struktur dla osób, których dane dotyczą, i opinii publicznej; oraz

- wykazanie w sposób satysfakcjonujący organowi nadzorczemu, że ich zadania i obowiązki nie powodują konfliktu interesów.

h) Wyznaczenie wewnętrznego inspektora ochrony danych

Rozporządzenie nie posługuje się nazwą znaną z polskiej ustawy z 1997 roku – „administratora bezpieczeństwa informacji - ABI", a sformułowaniem „inspektor ochrony danych".

Wyznaczenie wewnętrznego inspektora ochrony danych jest w rozumieniu art. 37 rozporządzenia obligatoryjne następujących przypadkach:

- przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;

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

- główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 rozporządzenia, oraz danych o sobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 rozporządzenia

Na uwagę zasługuje fakt (przy utożsamieniu obecnego pojęcia ABI a pojęciem inspektora ochrony), że rozporządzenie może położyć kres obecnie stosowanej praktyce „masowego ABI" tzn. osoby, która podejmuje się pełnienia funkcji ABI w kilkudziesięciu różnych podmiotach.

Powyższa konkluzja wynika z faktu, że rozporządzenie wyraźnie zastrzega wyjątkowe sytuacje, w których kilka podmiotów może wyznaczyć jednego inspektora, dotyczą one wyłącznie działania:

- w ramach grupy przedsiębiorstw (ale tylko pod warunkiem, że można będzie łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej), której definicja znajduje się w art. 4 oraz precyzowana jest w preambule do rozporządzenia

- w organie lub podmiocie publicznym (ale tylko z uwzględnieniem struktury organizacyjnej i wielkości)

- jako z rzeszenia lub podmioty reprezentujące określone kategorie administratorów (ale tylko w sytuacji, gdy nie zachodzą przesłanki określone w art. 37 ust. 1

i) Uregulowanie wieku pozwalającego na wyrażenie zgody na przetwarzanie danych w celu „usług społeczeństwa informacyjnego".

Rozporządzenie w art. 8 odnosząc się do „usług społeczeństwa informacyjnego" bezwzględnie zakazuje przetwarzania danych osobowych dzieci (jeżeli podstawą przetwarzania ma być zgoda, a nie np. realizacja zawartej umowy) poniżej 13 lat bez uzyskania zgody (lub jej zaaprobowania) rodzica lub opiekuna prawnego (domyślnie rozporządzenie ustala tą granicę na lat 16, ale zezwala państwu członkowskiemu na obniżenie tego wieku do 13 lat), i jednocześnie nakłada na administratora (np. operatora serwisu internetowego pozyskującego zgody) „podjęcie rozsądnych starań, by zweryfikować, czy osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem wyraziła zgodę lub ją zaaprobowała". Jednocześnie, rozporządzenie ustala, że osoba po ukończeniu 16 roku życia może sama wyrazić zgodę na przetwarzanie jej danych osobowych w przypadku usług społeczeństwa informacyjnego i nie jest konieczne jej zaaprobowanie przez jej opiekuna prawnego – państwo członkowskie natomiast nie może tej granicy podwyższyć (może ją jedynie obniżyć do 13 roku życia.)

3. Nowe definicje

Nietrudno zauważyć, że w roku 1995, gdy została przyjęta dyrektywa 95/46/WE ówczesny stan rozwoju technologicznego wiązał się z zupełnie innym kształtem prowadzenia działalności gospodarczej, naturalnym wynikiem postępującego rozwoju technologicznego jest pojawienie się w zawartym w artykule 4 rozporządzenia słowniku pojęć definicji nieznanych dyrektywie z 95 roku.

a) **Profilowanie -** dotyczy to np. coraz powszechniejszych sytuacji, w których serwisy zajmujące się sprzedażą internetową zbierają informacje o preferencjach konsumenta na podstawie których „przewidują" jego dalsze wybory (proponując mu przedmioty korelujące z jego preferencjami).

Rozporządzenie definiuje profilowanie jako „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"

Do profilowania odnoszą się także ustęp 60 preambuły, w którym wyrażone jest zobowiązanie administratora danych do poinformowania osoby, której dane dotyczą o fakcie profilowania, oraz konsekwencjach tego profilowania.

b) Pseudonimizacja - spseudonimizowane (do których odnoszą się także ust. 28 i 29 preambuły) dane osobowe to takie dane, które dopiero po posłużeniu się dodatkowymi informacjami (które muszą być przechowywane osobno) można przypisać konkretnej osobie fizycznej, inaczej mówiąc - są to takie dane, które po wstępnym ich zaprezentowaniu nie pozwalają ich przypisać konkretnej osobie fizycznej, ale po użyciu dodatkowych informacji jest to możliwe. Biorąc pod uwagę, że sama definicja danych osobowych posługuje się sformułowaniem „informacje o możliwej do zidentyfikowania osobie fizycznej", należy uznać, że dane osobowe poddane pseudonimizacji dalej pozostają danymi osobowymi, jest to jednak środek który pozwala zwiększyć bezpieczeństwo ich przetwarzania. Głównym założeniem pseudonimizacji (do której rozporządzenie w preambule „zachęca") jest wyodrębnienie dodatkowych informacji których celem jest jedynie umożliwienie przypisania konkretnych danych konkretnej osobie.

c) oraz d) Wprowadzenie odrębnych definicji „danych dotyczących zdrowia", oraz „danych genetycznych" – wcześniej, zarówno polska ustawa z 1997 roku jak i dyrektywa z 95 roku używały pojęcia „dane o stanie zdrowia" jako określenia jednej ze „szczególnych" kategorii danych osobowych (art. 8 ust. 1 dyrektywy z 1995 roku), w Polsce określanych jako tzw. „danych wrażliwych". Definicja zawarta rozporządzeniu jest znacznie bardziej szczegółowa – ale, co ciekawe, bardziej wyczerpująco została ona określona w ustępie 35 preambuły, niż w samym słowniku pojęć zawartym w artykule 4. Jako dane dotyczące zdrowia określono:

„(...)wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą. Do danych takich należą informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej, jak to określa dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE; numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych; informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych; oraz wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą , niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne in vitro."

e) Na szczególną uwagę zasługuje wprowadzenie definicji „danych biometrycznych" co powinno zwrócić uwagę np. pracodawców planujących wprowadzić zaawansowane technologicznie rozwiązania związane np. z monitorowaniem i regulowaniem dostępu pracowników do obiektów znajdujących się na terenach zakładów pracy, ponieważ rozporządzenie ustanawia generalny zakaz przetwarzania takich danych (chyba, że zajdzie wyjątek, o którym mowa w art. 9 ust. 2 rozporządzenia, np. realizacja szczególnych praw w dziedzinie prawa pracy, a prawo UE lub państwa członkowskiego na to pozwala). Jako dane biometryczne należy rozumieć takie dane osobowe

„(...)które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby takiej jak wizerunek twarzy lub dane daktyloskopijne(...)"

Pomimo istnienia generalnego zakazu przetwarzania danych biometrycznych, można wyobrazić sobie sytuację, w której np. właściciele obiektów rekreacyjnych np. siłowni, klubów fitness itd. Wprowadzą możliwość np. stosowania czytnika linii papilarnych zamiast zewnętrznej karty, karnetu itd. Jako podstawę prawną wskazując art. 9 ust. 2 lit. a rozporządzenia, który wskazuje że zakaz przetwarzania danych biometrycznych może być uchylony przez wyraźną zgodę osoby, której dane dotyczą do przetwarzania takich danych do konkretnego celu.

Rozporządzenie przewiduje jednak możliwość zablokowania możliwości przetwarzania danych biometrycznych na podstawie zgody przez prawo właściwego państwa członkowskiego.

f) W ustępie 22 preambuły zawarta jest definicja „jednostki organizacyjnej" jako podmiotu charakteryzującego się „skutecznym" i „faktycznym" prowadzeniem działalności przez „stabilne struktury", przy czym wyraźnie zastrzeżono, że nie musi on charakteryzować się odrębną osobowością prawną – nie musi to być odrębna spółka ani nawet oddział spółki. Z pojęciem jednostki organizacyjnej związana jest zawarta w słowniku z art. 4 definicja „głównej jednostki organizacyjnej" określenie to związane jest z sytuacją, w której dany podmiot posiada więcej niż jedną jednostkę organizacyjną na terenie UE, w takiej sytuacji za główną jednostkę będzie uznawana taka, w której „znajduje się centralna administracja w Unii" tego podmiotu – co do zasady, ponieważ rozporządzenie w dalszej części inaczej definiuje główną jednostkę organizacyjną „administratora" a inaczej „podmiotu przetwarzającego". Określanie właściwej jednostki organizacyjnej jako głównej będzie miało istotne znaczenie przy ustalaniu właściwości organów nadzorczych konkretnych państw członkowskich (w Polsce GIODO, a w innych państwach jego odpowiedników).
Na uwagę zasługuje także wprowadzenie definicji „grupy przedsiębiorstw" (składającej z przedsiębiorstwa kontrolującego i przedsiębiorstw kontrolowanych) gdzie jako decydujące kryterium wskazano między innymi kontrolowanie przetwarzania danych przedsiębiorstw przez przedsiębiorstwo kontrolujące.

g) Definicję zgody na przetwarzanie danych osobowych doprecyzowano w rozporządzeniu w ten sposób, że dodano wymaganą formę jej wyrażenia jako „okazanie woli w formie oświadczenia" lub „wyraźnego działania potwierdzającego" – co jest jedynie istotną zmianą w stosunku do dyrektywy, ponieważ w polskiej ustawie z 1997 roku zgoda utożsamiana była z oświadczeniem woli już od początku jej obowiązywania (art. 7 pkt 5 uodo).

4. Sankcje – kary pieniężne oraz inne środki, którymi dysponuje organ nadzorczy

Nowością wprowadzaną przez rozporządzenie jest nowy mechanizm nakładania kar pieniężnych za naruszenie przepisów rozporządzenia. Co do zasady będą one miały charakter administracyjny, z wyłączeniem Danii oraz Estonii, gdzie z uwagi na konstrukcję systemu prawnego będą one miały c harakter karny. Rozporządzenie dopuszcza ustanowienie przez państwa członkowskie także innego mechanizmu nakładania kar (np. ustanowienie przepisów karnych obok pieniężnych kar a dministracyjnych), pod warunkiem, że nie będzie to prowadziło do złamania zasady polegającej n a zakazie orzekania więcej niż raz w tej samej sprawie („ne bis in idem"). Podkreślone zostało przede wszystkim to, że nakładane kary pieniężne muszą być „skuteczne, proporcjonalne i odstraszające".

Należy podkreślić, że rozporządzenie wymienia rodzaje naruszeń, oraz określa górną granicę oraz kryteria ustalania administracyjnych kar pieniężnych, które GIODO jako organ nadzorczy będzie nakładał indywidualnie dla każdego przypadku.

Ustalenie czy (a jeżeli tak, to w jakim zakresie) pod kary pieniężne będą podlegały organy publiczne, rozporządzenie pozostawia konkretnym państwo członkowskim.

a) Nie tylko kary pieniężne.

Rozporządzenie w ustępie 148 Preambuły wskazuje, że w pewnych sytuacjach zamiast kary pieniężnej powinno zostać udzielone „upomnienie" – dotyczyć to powinno sytuacji, w których „(...)naruszenie jest n iewielkie lub jeżeli grożąca kara pieniężna stanowiłaby dla osoby fizycznej nieproporcjonalne o bciążenie(...)". W tym miejscu należy przytoczyć art. 58 ust. 2 rozporządzenia, którym wskazano inne n iż kary pieniężne środki, jakimi GIODO jako organ nadzorczy może się posługiwać (zamiast kar pieniężnych, lub oprócz nich) do takich narzędzi należą:

- wydawanie ostrzeżeń administratorowi lub podmiotowi przetwarzającemu w związku z możliwością naruszenia przepisów rozporządzenia przez planowane operacje przetwarzania.

- udzielanie upomnień administratorowi lub podmiotowi przetwarzającemu w przypadku naruszenia przepisów rozporządzenia przetwarzania przez operacje przetwarzania

- nakazanie administratorowi lub podmiotowi przetwarzającemu spełnienia żądania osoby, której dane dotyczą, wynikającego z praw przysługujących jej na mocy rozporządzenia

- nakazanie administratorowi lub podmiotowi przetwarzającemu dostosowania operacji przetwarzania do przepisów rozporządzenia, a w stosownych przypadkach wskazanie sposobu i terminu;

- nakazanie administratorowi zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych;

- wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania

- nakazanie na mocy sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarza nia oraz nakazanie powiadomienia o tych czynnościach odbiorców, którym dane osobowe ujawniono;

- cofnięcie certyfikacji lub nakazanie podmiotowi certyfikującemu cofnięcia certyfikacji udzielonej na mocy art. 42 lub 43, lub nakazanie podmiotowi certyfikującemu nieudzielania certyfikacji, jeżeli jej wymogi nie są spełnione lub przestały być spełniane;

- nakazanie zawieszenia przepływu danych do odbiorcy w państwie trzecim lub do organizacji międzynarodowej.

b) Kryteria decydowaniu o zastosowaniu kar pieniężnych lub innych środków.

Rozporządzenie wskazuje, że przy ocenie, czy w danej sytuacji wystarczające będzie nałożenie przez organ nadzorczy (w Polsce będzie to GIODO) kary pieniężnej czy też zastosowanie innego środka (np. upomnienia) należy zwrócić uwagę na takie elementy jak:

- charakter, wagę oraz czas trwania naruszenia, przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób, których dane dotyczą, oraz rozmiaru poniesionej przez nie szkody;
- umyślny lub nieumyślny charakter naruszenia;
- działania podjęte dla zminimalizowania szkody,
- stopień odpowiedzialności z uwzględnieniem środków technicznych i organizacyjnych przez nich wdrożonych
- wszelkie mające znaczenie wcześniejsze naruszenia,
- stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków
- kategorie danych osobowych, których dotyczyło naruszenie
- sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, w szczególności, czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosili naruszenie
- przestrzeganie środków nałożonych na administratora lub podmiot przetwarzający (jeżeli były wcześniej nałożone),
- stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji
- wszelkie inne obciążające lub łagodzące czynniki mające zastosowanie do okoliczności sprawy, takie jak osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty

c) Wysokość kar pieniężnych.

Karę pieniężną w wysokości do 10 000 000 euro, a w przypadku przedsiębiorstwa w wysokości do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa – stosuje się za naruszenia obowiązków administratora (lub podmiotu przetwarzającego dane) o których mowa w:

- art. 8, obowiązki związane z przetwarzaniem danych osobowych dziecka poniżej 16 lat (państwo członkowskie może obniżyć ten próg do 13 lat) w przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku bez wyrażonej lub zaaprobowanej zgody przez osobę sprawującą władzę rodzicielską lub opiekę nad dzieckiem. Należy pamiętać, że administrator danych jest zobowiązany podjąć „rozsądne starania" by zweryfikować, czy osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem wyraziła zgodę lub ją zaaprobowała.

- art. 11, obowiązki w związane z przetwarzaniem niewymagającym identyfikacji

- art. 25, obowiązki związane z wdrożeniem odpowiednich środków technicznych i organizacyjnych (pseudonimizacja, minimalizacja) w celu zabezpieczenia danych między innymi przed dostępem osób nieuprawnionych oraz zapewnienia realizacji zasady adekwatności przetwarzanych danych (by przetwarzać tylko te dane, które są niezbędne do realizacji określonych celów).

- art. 26, obowiązki związane z uzgodnieniem zakresów odpowiedzialności współadministratorów danych

- art. 27, obowiązki związane z wyznaczeniem na piśmie przedstawiciela w Unii przez administratora danych lub podmiot przetwarzający niemający jednostek organizacyjnych w Unii.

- art. 28, obowiązki związane z właściwym uregulowaniem relacji pomiędzy administratorem danych a podmiotem przetwarzającym dane w jego imieniu

- art. 29, obowiązki związane z przetwarzaniem danych przez podmioty przetwarzające oraz osoby działające z upoważnienia mające dostęp do danych osobowych wyłącznie na polecenie administratora danych

- art. 30, obowiązki związane z prowadzeniem rejestru czynności przetwarzania danych osobowych przez administratora danych

- art. 31, obowiązki związane ze współpracą przez administratora danych oraz podmiot przetwarzający z organem nadzorczym

- art. 32, obowiązki związane z wdrożeniem odpowiednich środków organizacyjnych i technicznych w celu zapewnienia stopnia bezpieczeństwa odpowiadającemu ryzyku (pseudonimizacja, szyfrowanie, zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego, regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania)

- art. 33, obowiązki związane ze zgłoszeniem naruszenia ochrony danych osobowych do organu nadzorczego w ciągu 72 godzin oraz dokumentowanie naruszenia

- art. 34, obowiązki związane z zawiadomieniem osoby, której dane dotyczą o fakcie naruszenia ochrony danych osobowych

- art. 35, obowiązki związane z oceną skutków planowanych operacji przetwarzania dla ochrony danych osobowych wedle przewidzianej w rozporządzeniu procedury

- art. 36, obowiązki związane z koniecznością konsultowania się z organem nadzorczym, w związku z efektem oceny skutków dla ochrony danych, o której stanowi art. 35 rozporządzenia

- art. 37, obowiązki związane z wyznaczeniem inspektora ochrony danych

- art. 38, obowiązki związane z zapewnieniem niezależności oraz umożliwienia swobodnego wykonywania czynności przez inspektora ochrony danych

- art. 39, obowiązki związane z wypełnianiem przez inspektora ochrony danych swoich obowiązków

- art. 42 oraz 43 obowiązki związanych z realizacją oraz zapewnieniem przejrzystości przyjętego przez administrator lub podmiot przetwarzający mechanizmu certyfikacji

- obowiązków podmiotu certyfikującego, o których mowa w art. 42 oraz 43;

- obowiązków podmiotu monitorującego, o których mowa w art. 41 ust. 4;

Karę pieniężną w wysokości do 20 000 000 euro, a w przypadku przedsiębiorstwa w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa - stosuje się za naruszenia o których mowa w:

- art. 5, 6, 7 oraz 9, w zakresie podstawowych zasad przetwarzania, w tym warunków zgody

- art. 12-22, w zakresie praw osób, których dane dotyczą

- art. 44-49, w zakresie przekazywania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej,

- art. 85- 91, w zakresie wykonywania obowiązków wynikających ze szczegółowych uregulowań państw członkowskich, wydanych w granicach i na podstawie art. 85-91 (rozdziału IX rozporządzenia)]

- art. 58, w zakresie nieprzestrzegania nakazu, tymczasowego lub ostatecznego ograniczenia przetwarzania lub zawieszenia przepływu danych orzeczonego przez organ nadzorczy lub nieza-pewnienia dostępu organowi nadzorczemu

Należy zwrócić uwagę na ograniczenie wysokości kary pieniężnej zawarte w art. 83 ust. 3 rozporządzenia które stanowi, że całkowita wysokość nałożonej kary pieniężnej w przypadku naruszenia (umyślnie lub nieumyślnie) kilku przepisów w związku z tymi samymi lub powiązanymi operacjami przetwarzania nie może przekroczyć kary za najpoważniejsze naruszenie.

5. Możliwość ustanowienia przez państwa członkowskie przepisów szczególnych w odniesieniu określonych przypadkach

Rozporządzenie wprowadza w rozdziale IX możliwość szczegółowego uregulowania przepisów dotyczących ochrony danych osobowych w poszczególnych przypadkach, do których należą:

a) Przetwarzanie danych przez kościoły oraz związki lub wspólnoty wyznaniowe, przy czym należy zauważyć, że jeżeli w danym państwie członkowskim realizują one cele ochrony danych osobowych poprzez przepisy szczególne, to ten stan może trwać także po wejściu w życie rozporządzenia, ale wyłącznie pod warunkiem dostosowania tych zasad do reguł określonych w rozporządzeniu. Rozporządzenie dopuszcza także ustanowienie odrębnego organu nadzorczego dla takich podmiotów, o ile spełniał będzie on kryteria określone w rozdziale VI rozporządzenia.

b) Kontrolowanie przetwarzania danych osobowych objętych tajemnicą zawodową (np. dziennikarską, adwokacką), rozporządzenie przewiduje możliwość ustanowienia szczególnych ram wykonywania przez organ nadzorczy w danym państwie członkowskim w czynności kontrolnych co do danych objętych taką tajemnicą, w zakresie:

„(...)uzyskiwania od administratora i podmiotu przetwarzającego dostępu do wszelkich danych osobowych i wszelkich informacji niezbędnych organowi nadzorczemu do realizacji swoich zadań; oraz uzyskiwanie dostępu do wszystkich pomieszczeń administratora i podmiotu przetwarzającego, w tym do sprzętu i środków służących do przetwarzania danych, zgodnie z procedurami określonymi w prawie unijnym lub w prawie państwa członkowskiego."

c) przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, rozporządzenie w art. 89 szczególna uwagę zwraca na minimalizację oraz (o ile jest to możliwe) pseudonimizację danych. Przewiduje także możliwość zastosowania w prawie krajowym wyłączeń od uprawnień nadanych osobom, których dane dotyczą, o których mowa w art. 15, 16, 18 i 21 rozporządzenia. Zwrócono również szczególną uwagę na zapewnienie

d) przetwarzanie danych osobowych w kontekście zatrudnienia, art. 88 rozporządzenia przewiduje możliwość ustanowienia przez prawo danego państwa członkowskiego „bardziej szczegółowych przepisów mających zapewnić ochronę praw i wolności" przy przetwarzaniu danych w szczególności w związku z procedurami rekrutacyjnymi oraz wykonywaniem umowy o pracę, ale także i *„(...)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.(...)"*

Zwrócono również szczególną uwagę, by ustalone w w tym trybie przepisy zapewniały *„(...) przejrzystość przetwarzania, przekazywania danych osobowych w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą oraz systemów monitorujących w miejscu pracy.(...)"*

e) przetwarzanie krajowego numeru identyfikacyjnego, rozporządzenie wprowadza możliwość ustanowienia przez prawo danego państwa członkowskiego szczególnych warunków przetwarzania krajowego numeru identyfikacyjnego (w Polsce będzie nim PESEL, w innych państwach członkowskich jego odpowiedniki).

f) przetwarzanie danych zawartych w dokumentach urzędowych, które posiada organ lub podmiot publiczny lub podmiot prywatny w celu wykonania zadania realizowanego w interesie publicznym, rozporządzenie w art. 86 przewiduje, że dane osobowe zawarte tego rodzaju dokumentach mogą zostać ujawnione (jeżeli będzie to przewidziane przez prawo państwa członkowskiego) *„(...) dla pogodzenia publicznego dostępu do dokumentów urzędowych z prawem do ochrony danych osobowych(...)"*

g) przetwarzanie danych osobowych w związku wolnością wypowiedzi i informacji, art. 85 rozporządzenia nakłada na państwa członkowskie obowiązek przyjęcia przepisów, których celem ma być pogodzenie – a jednej strony zasad ochrony danych osobowych, a z drugiej wolności wypowiedzi i informacji (w tym potrzeb dziennikarskich oraz do celów wypowiedzi akademickiej, artystycznej lub literackiej). Rozporządzenie przewiduje przy tym ogólne ramy określając, wyjątki określonych reguł w nim przewidziany mogą być zastosowane tylko o tyle, o ile są niezbędne do realizacji wyżej wskazanego celu.

Dziękujemy za Państwa zaufanie!

Jeśli są Państwo zainteresowani audytem oraz wdrożeniami systemu ochrony danych zgodnie z obowiązującymi przepisami, zapraszamy do kontaktu pod mailem:

biuro@rbdo.pl lub telefonem: (22) 487 86 70