OMNI MODO

GDPR

Wybrane zagadnienia z unijnego ogólnego rozporządzenia o ochronie danych osobowych

Kilka słów wstępu

W dniu 14 kwietnia 2016 r. Parlament Europejski zatwierdził Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych, zwane potocznie General Data Protection Regulation (GDPR). Tym samym zmiana systemu ochrony danych osobowych została ostatecznie przesądzona. Z powodu dużych i kosztowych zmian Parlament dał Państwom Członkowskim ponad 2-letni okres dostosowania się do nowej rzeczywistości.

Mam przyjemność przedstawić Państwu efekt prac zespołu naszych specjalistów. Dokonali oni dogłębnej analizy nowych przepisów, na podstawie której przygotowano dla Państwa niniejszą publikację. Dobór artykułów nie jest przypadkowy. Przedstawione poniżej zagadnienia mogą mieć największy wpływ na prowadzoną przez Państwa działalność gospodarczą.

Serdecznie zapraszam do przeczytania niniejszej publikacji

Tomasz Osiej

Radca Prawny, Europejski Rzecznik Patentowy

Tel.: +48 505 165 660 e-mail: t.osiej@omnimodo.com.pl

Omni Modo
Aleja Jerzego Waszyngtona 40A, 1p.
03-910 Warszawa
NIP 113-060-77-41

tel./fax: 22 616 25 70
e-mail: omnimodo@omnimodo.com.pl
www.omnimodo.com.pl

Spis treści

Skróty

ABI – Administrator bezpieczeństwa informacji – podmiot, o którym mowa w art. 36a UODO.

ADO – Administrator danych – organ, jednostka organizacyjna, podmiot lub osoba, o których mowa w art. 3 U0ODO, decydujący o celach i środkach przetwarzania danych osobowych (zgodnie z art. 7 pkt 4 UODO.

DPO – Data Protection Officer – podmiot, o którym mowa w 37 GDPR.

GDPR – General Data Protection Regulation, Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych.

GIODO – Generalny Inspektor Ochrony Danych Osobowych – organ do spraw ochrony danych osobowych, o którym mowa w art. 8 UODO.

UODO – Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U.2016 poz.922 j.t.

Omni Modo
Aleja Jerzego Waszyngtona 40A, 1p.
03-910 Warszawa
NIP 113-060-77-41

tel./fax: 22 616 25 70
e-mail: omnimodo@omnimodo.com.pl
www.omnimodo.com.pl

Marcin Cwener

Zgłaszanie incydentów bezpieczeństwa do GIODO
Analiza art. 33 GDPR

GDPR nakłada na administratorów danych szereg nowych praw i obowiązków. Jednym z nich jest obowiązek zawiadomienia organu nadzorczego o naruszeniu przetwarzania danych osobowych, zwany obowiązkiem notyfikacji naruszeń (*data breach notification*).

Celem niniejszego artykułu jest analiza instytucji, w szczególności próba odpowiedzi na pytanie w jaki sposób administratorzy danych (oraz administratorzy bezpieczeństwa informacji) mogą przygotować się do przeprowadzenia ewentualnej notyfikacji, jeszcze przed rozpoczęciem obowiązywania przepisów GDPR.

Notyfikacja czyli…?

Zgodnie z art. 33 ust. 1 GDPR, 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, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Przede wszystkim podkreślić należy, że norma zawarta w ww. przepisie, **nie nakłada na** administratorów danych obowiązku informowania organu nadzorczego (w Polsce na chwilę obecną takim organem jest GIODO) o **jakimkolwiek incydencie związanym z przetwarzaniem danych osobowych.** Notyfikacja powinna być efektem naruszenia ochrony danych osobowych, zgodnie zaś z definicją legalną zawartą w art. 4 pkt 12 GDPR, za naruszenie ochrony danych osobowych uznaje się **naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych**. Zatem

Omni Modo
Aleja Jerzego Waszyngtona 40A, 1p.
03-910 Warszawa
NIP 113-060-77-41

tel./fax: 22 616 25 70
e-mail: omnimodo@omnimodo.com.pl
www.omnimodo.com.pl

nie w każdym przypadku wykrycie na skutek bieżącego nadzoru nad przetwarzaniem danych osobowych (np. w związku z realizacją zasady *privacy by design)*. **Uchybienia przepisom regulującym ochronę danych osobowych będzie wiązało się z obowiązkiem notyfikacji**. Dla przykładu naruszeniem ochrony danych osobowych **nie będzie** błędne (niepełne) wypełnienie obowiązku informacyjnego, bądź wadliwie skonstruowanie zgody jako podstawy prawnej przetwarzania danych osobowych (co nie zmienia faktu, że tego typu uchybienia w przypadku wykrycia przez organ nadzoru, mogą wiązać się z nałożeniem kary w wysokości nawet do 20 000 000 EUR).

Mając na uwadze powyższe zastrzeżenie, przyjąć należy, że obowiązek notyfikacji, jest związany z takim zdarzeniem, którego efektem jest **naruszenie bezpieczeństwa przetwarzanych danych**. Istotnym jest przy tym, iż naruszenie powinno prowadzić do wystąpienia określonego w art. 4 pkt 12 GDPR skutku (np. utracenia danych), przy czym nie ma znaczenia, czy naruszenie związane było z działaniem przypadkowym czy niezgodnym z prawem.

Pomocna dla zrozumienia sensu ograniczenia obowiązku notyfikacji wyłącznie do przypadków związanych z incydentem bezpieczeństwa będzie analiza motywu 85 GDPR. Motyw ten określa, że brak odpowiedniej i szybkiej reakcji na naruszenie ochrony danych (jak powyżej wskazano, rozumianego jako naruszenie bezpieczeństwa przetwarzanych danych), może skutkować powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych, takich **jak utrata kontroli nad własnymi danymi, ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa** itp.

Obowiązek notyfikacji jest zatem elementem usuwania skutków incydentów bezpieczeństwa mogących mieć istotny wpływ na interesy osoby fizycznej i wynika z powszechnie akceptowanej i, jak się wydaje, oczywistej zasady bezpieczeństwa przetwarzania danych[1].

Termin i treść zgłoszenia

Obowiązek zgłoszenia naruszenia powinien zostać zrealizowany **bez zbędnej zwłoki, w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia**. W przypadku przekroczenia ww. terminu administrator będzie zobowiązany do wyjaśnienia

[1] Por. http://www2.deloitte.com/nl/nl/pages/risk/articles/the-general-data-protection-regulation.html

Omni Modo
Aleja Jerzego Waszyngtona 40A, 1p.
03-910 Warszawa
NIP 113-060-77-41

tel./fax: 22 616 25 70
e-mail: omnimodo@omnimodo.com.pl
www.omnimodo.com.pl

GIODO przyczyn opóźnienia. Warto jednak pamiętać, że nieopłacalnym może być celowe unikanie spełnienia obowiązku notyfikacji, gdyż zgodnie z art. 83 ust. 4 lit a GDPR, działanie takie będzie zagrożone administracyjną karą pieniężną do 10 000 000 EUR, bądź 2% całkowitego rocznego światowego obrotu.

Zgłoszenie naruszenia do GIODO **powinno zawierać:**

a) opis charakteru naruszenia, w tym w miarę możliwości wskazywać kategorię i przybliżoną liczbę osób, których dane dotyczą,

b) imię i nazwisko oraz dane kontaktowe inspektora ochrony danych (ABI),

c) opis możliwych konsekwencji naruszenia,

d) opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych oraz minimalizowaniu negatywnych skutków naruszenia.

Warto jednak pamiętać, że na dzień dzisiejszy nie można jednoznacznie przesądzić, iż do 25 maja 2018 r. nie zostaną przyjęte przepisy, które w szczegółowy sposób określą formę i tryb mający zastosowanie przy realizacji obowiązku notyfikacji. Na okoliczność taką wskazuje motyw 88 GDPR.

Może jednak naruszenie nie jest poważne?

Prawdziwym wyzwaniem dla administratorów danych, ale jak sądzę, również dla organów nadzoru, będzie wykładnia i praktyczne zastosowanie wyłączenia od obowiązku notyfikacji, w przypadku w którym wykryte naruszenie bezpieczeństwa będzie związane z niewielkim prawdopodobieństwem zaistnienia ryzyka naruszenia praw lub wolności osób fizycznych. Mając na uwadze, iż niedopełnienie obowiązku notyfikacji skutkować może nałożeniem przez organ finansowej kary administracyjnej, ocena prawdopodobieństwa wystąpienia ryzyka naruszenia praw i wolności nabiera szczególnego znaczenia. Wydaje się, że poza zdrowym rozsądkiem oraz pro klienckim podejściem, administratorzy danych przy dokonywaniu ww. oceny powinni kierować się wytycznymi organów nadzorczych krajów UE (nie tylko GIODO), jak i innych instytucji opiniodawczych. Jako przykład można wskazać niezwykle ważną opinię Grupy Roboczej Art. 29 na temat powiadamiania o przypadkach naruszenia danych osobowych[2], w treści której Grupa zawarła szereg przykładów naruszeń, które mogą wywierać niekorzystny wpływ na osoby, których

[2] http://www.giodo.gov.pl/1520203/id_art/7788/j/pl/

Omni Modo
Aleja Jerzego Waszyngtona 40A, 1p.
03-910 Warszawa
NIP 113-060-77-41

tel./fax: 22 616 25 70
e-mail: omnimodo@omnimodo.com.pl
www.omnimodo.com.pl

dane dotyczą, oraz przykładowe działania zabezpieczające, dzięki którym można byłoby ograniczyć ryzyko, gdyby zostały one zawczasu wdrożone.

Notyfikacja już funkcjonuje

Pomimo, iż ustawa o ochronie danych osobowych, ani dyrektywa 95/46/WE nie przewidywała obowiązku notyfikacji naruszeń do GIODO, jednak sama koncepcja nie stanowi bezwzględnego *novum* w polskim porządku prawnym. Pomijając wytyczne wzywające do dobrowolnego zgłaszania naruszeń wydawane przez Grupę Roboczą Art. 29[3], przywołać należy obowiązek notyfikacji naruszeń określony w art. 174a ustawy Prawo telekomunikacyjne, który wiąże **dostawców powszechnie dostępnych usług telekomunikacyjnych**. Podobnie jak w przypadku art. 33 GDPR, obowiązek wskazany w Prawie telekomunikacyjnym odnosi się do naruszeń bezpieczeństwa danych na skutek przypadkowego lub bezprawnego zniszczenia, utraty, zmiany, nieuprawnionego ujawnienia lub dostępu do danych osobowych przetwarzanych przez przedsiębiorcę telekomunikacyjnego. Przedsiębiorca taki jest zobligowany do poinformowania o zdarzeniu GIODO w terminie 3 dni od stwierdzenia naruszenia.

Jak się przygotować?

Próba odpowiedzi na to pytanie nie jest łatwa. Wydaje się jednak, że najlepszą metodą będzie wdrożenie w organizacji (tam gdzie to jeszcze nie funkcjonuje) rejestru incydentów związanych z bezpieczeństwem danych, oraz prowadzenie pełnej dokumentacji związanej z postępowaniem zmierzającym do usunięcia skutków uchybień, w szczególności warto zapewnić, aby dokumentacja zawierała elementy, które będą obligatoryjne w przyszłej notyfikacji, zwłaszcza opis możliwych konsekwencji naruszenia, oraz środków podjętych celem neutralizacji efektów incydentu.

[3] Por. D. Lubasz, Europejska reforma ochrony danych osobowych – nowe obowiązki administratorów o ogólnym rozporządzeniu o ochronie danych, w: E. Bielak – Jomma, D. Lubasz (red.) Polska i europejska reforma ochrony danych osobowych, Wolters Kluwer, Warszawa 2016

Omni Modo
Aleja Jerzego Waszyngtona 40A, 1p.
03-910 Warszawa
NIP 113-060-77-41

tel./fax: 22 616 25 70
e-mail: omnimodo@omnimodo.com.pl
www.omnimodo.com.pl

7 SYTUACJI, W KTÓRYCH SPOTKASZ SIĘ Z ORGANEM NADZORCZYM

1. Rejestrowanie czynności przetwarzania

Administrator lub procesor prowadzą rejestr czynności przetwarzania danych osobowych. Podmioty te udostępniają rejestr na żądanie organu nadzorczego.

2. Współpraca z organem nadzorczym

Administrator i procesor na żądanie współpracują z organem nadzorczym w ramach wykonywania przez niego zadań.

3. Zgłaszanie naruszeń

W przypadku naruszenia ochrony danych osobowych administrator – nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.

4. Zawiadamianie osoby o naruszeniu

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Z uwagi na stopień naruszenia organ nadzorczy może zażądać od zgłaszającego podjęcia czynności zabezpieczających dane.

5. Uprzednie konsultacje

W przypadku ryzyka dla bezpieczeństwa danych przed rozpoczęciem przetwarzania administrator konsultuje się z organem nadzorczym. Organ nadzorczy udziela administratorowi pisemnego zalecenia co do przetwarzania danych.

6. ABI/ DPO jako punkt kontaktowy

Administrator lub procesor publikują dane kontaktowe inspektora ochrony danych i zawiadamiają o nich organ nadzorczy. Dodatkowo jednym z zadań inspektora ochrony danych jest współpraca z organem nadzorczym oraz pełnienie funkcji punktu kontaktowego dla niego w kwestiach związanych z przetwarzaniem danych.

7. Wniesienie skargi

Osoba, której dane dotyczą ma prawo wnieść skargę do organu nadzorczego, jeżeli sądzi, że przy przetwarzaniu jej danych osobowych doszło do złamania przepisów rozporządzenia.
Organ nadzorczy – w ramach prowadzonego postępowania – odbiera wyjaśnienia od podmiotu, którego skarga dotyczy.

Marta Bargiel-Kaflik

Powierzenie przetwarzania danych w GDPR[4]

Prawodawca europejski w sposób szczególny uregulował w GDPR pozycję podmiotu przetwarzającego w imieniu administratora dane (przez doktrynę nazywanego „procesorem") oraz dość precyzyjnie opisał prawa i obowiązki pomiędzy tymi podmiotami.

Warto wspomnieć, że aktualnie obowiązująca ustawa o ochronie danych osobowych, skąpo odnosi się do tych relacji, pozostawiając sporo pola do interpretacji podmiotom zaangażowanym w procesy przetwarzania danych oraz podmiotom orzekającym co do legalności tych procesów (GIODO, sądy administracyjne).

Kilka słów o tym jak na gruncie GDPR powierzyć dane do przetwarzania

Przepis art. 28 ust. 1 GDPR stanowi, że jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą. GDPR nakłada zatem na administratora obowiązek **dołożenia szczególnej staranności** przy wyborze kontrahenta mającego w jego imieniu przetwarzać dane. Jak się wydaje, ocena spełniania przez „procesora" wymogów przewidzianych ww. przepisem GDPR, mogłaby zostać dokonana po przeprowadzeniu przez administratora danych kontroli stosowanych sposobów zabezpieczania danych. Trend przeprowadzania audytów i kontroli u kontrahentów, którym powierza się dane do przetwarzania staje się obecnie na rynku outsourcingu tego typu usług coraz bardziej zauważalny. Brak jednak wyraźnych przepisów UODO odnoszących się do tej możliwości powoduje, że „procesorzy" niejednokrotnie blokują

[4] Artykuł pierwotnie został opublikowany pod tym samym tytułem na portalu e-ochronadanych.pl

Omni Modo
Aleja Jerzego Waszyngtona 40A, 1p.
03-910 Warszawa
NIP 113-060-77-41

tel./fax: 22 616 25 70
e-mail: omnimodo@omnimodo.com.pl
www.omnimodo.com.pl

możliwość ich przeprowadzania. Biorąc pod uwagę olbrzymią ilość podmiotów przetwarzających w Polsce dane na zlecenie, zauważyć trzeba, że relatywnie niewielka ich część wdrożyła w organizacjach ochronę danych na takim poziomie, że perspektywa przeprowadzenia przez kontrahenta kontroli, od której być może uzależniona jest dalsza współpraca, nie powoduje ich sprzeciwu.

Umieszczenie expressis verbis, w art. 28 ust. 3 lit. h GDPR, **obowiązku umożliwienia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzania audytów**, powoduje, że stan niepewności prawnej co do powyżej wspomnianego uprawnienia administratora został w GDPR zniesiony. Pod rządami GDPR sygnał od administratora o potrzebie przeprowadzenia kontroli przestanie być traktowany jako prośba, a zacznie być traktowany jako „propozycja nie do odrzucenia". Zmianę tę należy, w mojej opinii, ocenić pozytywnie. Nie powinno ulegać wątpliwości, że po stronie administratora istnieje wyraźna potrzeba do przeprowadzania takich kontroli. To na jego barkach ciąży bowiem zdecydowany ciężar odpowiedzialności, tak prawnej, jak i biznesowej, za przetwarzane dane.

Elementy umowy powierzenia

Administrator danych, na gruncie GDPR, będzie mógł powierzyć do przetwarzania dane na podstawie umowy lub *innego instrumentu prawnego*. Zarówno umowa, jak i wspomniany *inny instrument prawny* będą musiały precyzyjnie określać szeroko rozumiane okoliczności powierzenia, a także zawierać wymienione przez GDPR szczegółowe deklaracje, co do obowiązków podmiotu przetwarzającego.

Zgodnie z art. 28 ust. 3 GDPR, administrator będzie musiał precyzyjnie określić:

1. przedmiot i czas trwania przetwarzania;
2. charakter i cel przetwarzania;
3. rodzaj danych osobowych oraz kategorie osób, których dane dotyczą;
4. obowiązki i prawa administratora.

Jednocześnie, umowa lub *inny instrument prawny* będą musiały stanowić w szczególności, że podmiot przetwarzający:

- przetwarza dane osobowe wyłącznie na **udokumentowane polecenie administratora;**

Omni Modo
Aleja Jerzego Waszyngtona 40A, 1p.
03-910 Warszawa
NIP 113-060-77-41

tel./fax: 22 616 25 70
e-mail: omnimodo@omnimodo.com.pl
www.omnimodo.com.pl

- zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do **zachowania tajemnicy** lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
- **wdroży odpowiednie środki techniczne i organizacyjne,** aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych (środki te mogą obejmować np. pseudonimizację i szyfrowanie danych osobowych, zapewnienie poufności, integralności, dostępności i odporności systemów i usług przetwarzania, przywracanie dostępności danych w razie incydentu fizycznego lub technicznego, regularne testowanie i ocenianie skuteczności ww. środków);
- pomaga administratorowi wywiązać się z obowiązku **odpowiadania na żądania osoby**, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III GDPR (a więc wspiera w realizacji uprawnień osoby o charakterze informacyjnym, korekcyjnym i zakazowym);
- **pomaga administratorowi** w zabezpieczaniu danych, zgłaszaniu naruszeń organowi nadzorczemu, zawiadamianiu osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych);
- po zakończeniu świadczenia usług, zależnie od decyzji administratora, **usuwa lub zwraca wszelkie dane osobowe** na jego rzecz oraz usuwa wszelkie ich istniejące kopie;
- **umożliwia przeprowadzanie audytów** i przyczynia się do nich.

Jak widać, ilość elementów umowy powierzenia została przez GDPR bardzo wzbogacona. Administratorzy danych, którzy temat powierzania danych do przetwarzania traktowali poważnie, włączali jednak już wcześniej do umów z procesorami znaczną ilość ww. postanowień, pomimo tego, że UODO dla skuteczności umowy ich nie przewidywała.

Omni Modo
Aleja Jerzego Waszyngtona 40A, 1p.
03-910 Warszawa
NIP 113-060-77-41

tel./fax: 22 616 25 70
e-mail: omnimodo@omnimodo.com.pl
www.omnimodo.com.pl

Forma umowy powierzenia

Kolejnym ciekawym doprecyzowaniem, które pojawiło się w GDPR, jest jasne wskazanie, że *umowa lub inny akt prawny, o których mowa w ust. 3 i 4, mają formę pisemną, w tym formę elektroniczną* [5] . Na marginesie wspomnieć też trzeba, że oficjalne tłumaczenie GDPR na język polski zawiera błąd polegający na odesłaniu w ww. przepisie nie do ust. 3 i 4 artykułu 28 ale do art. 3 i 4 GDPR. Traktować tą nieścisłość należy jako oczywistą omyłkę. W wersji anglojęzycznej GDPR użyto bowiem w odniesieniu do wspomnianych jednostek redakcyjnych zwrotu „paragraph", który powinien być tłumaczony na język polski jako ustęp, a nie jako artykuł.

„Dalsze powierzenie" danych do przetwarzania

GDPR w sposób nie pozostawiający wątpliwości odniósł się ponadto do zlecania przez podmiot przetwarzający dane przetwarzania ich przez „inny podmiot przetwarzający". Aktualnie, UODO nie przewiduje wprost możliwości „podpowierzania danych" przez ich „procesora". UODO stanowi bowiem, że to „*administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych*"[6]. Interpretując literalnie przepisy UODO można dojść do przekonania, że uprawnienie do powierzania przetwarzania danych przysługuje jedynie ich administratorowi. Doktryna i orzecznictwo, opierając się na wykładni celowościowo-funkcjonalnej, wypracowały jednak stanowisko, z którego wynika, że podmiot przetwarzający dane może je powierzyć do „dalszego" przetwarzania innemu podmiotowi, po uzyskaniu aprobaty administratora danych.

Prawodawca unijny zauważając potrzebę precyzyjnego uregulowania tej kwestii, zawarł w GDPR postanowienie, że:

„podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody przetwarzający informuje administratora o wszelkich zamierzonych zmianach

[5] art. 28 ust. 9 GDPR
[6] art. 31 ust. 1 UODO

Omni Modo
Aleja Jerzego Waszyngtona 40A, 1p.
03-910 Warszawa
NIP 113-060-77-41

tel./fax: 22 616 25 70
e-mail: omnimodo@omnimodo.com.pl
www.omnimodo.com.pl

dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian"[7].

Mamy tutaj więc do czynienia z sytuacją, w której **administrator danych może pisemnie wprost przewidzieć jakiemu „podprocesorowi" dane mogą być, w razie potrzeby, powierzone** do przetwarzania przez podmiot przetwarzający bądź też może **pisemnie przewidzieć możliwość takiego „dalszego powierzenia"** przez podmiot przetwarzający dane, nie wskazując przy tym konkretnie jaki podmiot finalnie dane może przetwarzać. W tej ostatniej sytuacji podmiot przetwarzający dane, noszący się z zamiarem „dalszego powierzenia" danych, zobowiązany jest do zasygnalizowania administratorowi tej okoliczności oraz umożliwienia mu wypowiedzenia się w tym przedmiocie. Niedopuszczalną jest więc sytuacja, w której administrator ma przekazywaną informację ale nie jest mu gwarantowany czas na podjęcie władczej decyzji co do takiego „dalszego powierzenia". Wydaje się, że czas oczekiwania na decyzję administratora w tym przedmiocie powinien być sztywno określony w umowie powierzenia.

Dodatkowo, przepis art. 28 ust. 4 GDPR stanowi, że:

„jeżeli do wykonania w imieniu administratora konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego – te same obowiązki ochrony danych jak między administratorem a podmiotem przetwarzającym".

Z powyższego wynika więc, że w zakresie obowiązków związanych z zabezpieczaniem danych podmiot, któremu podmiot przetwarzający „podpowierzył" dane do przetwarzania zobowiązany jest do wdrożenia takich środków zabezpieczających, jakie mają być wdrożone przez podmiot „podpowierzający". W sytuacji, w której „podprocesor" nie wywiązałby się z tego obowiązku, odpowiedzialność wobec administratora za skutki tego zaniechania ponoszona ma być przez podmiot „podpowierzający" dane. Pojawić się zatem może pytanie, czy na zasadzie analogii, podmioty „podpowierzające" dane nie będą się decydowały na uprzednią kontrolę swoich kontrahentów, którym „podpowierzają" dane.

[7] art. 28 ust. 2 GDPR

Omni Modo
Aleja Jerzego Waszyngtona 40A, 1p.
03-910 Warszawa
NIP 113-060-77-41

tel./fax: 22 616 25 70
e-mail: omnimodo@omnimodo.com.pl
www.omnimodo.com.pl

Podsumowanie

Zmiany jakie GDPR wprowadził do relacji zachodzących pomiędzy administratorem danych i ich „procesorem", względnie „podprocesorem", ocenić należy pozytywnie. Odnosząc uregulowania GDPR do obowiązującej UODO nie sposób nie zauważyć, że dotychczasowe rozwiązania nie były precyzyjne, co rodziło przez wiele lat szereg problemów interpretacyjnych. GDPR traktuje procesora nie jako podmiot, który stoi po przeciwnej niż administrator danych stronie barykady, ale jako podmiot, który aktywnie wspierać ma lub też wręcz inicjować procesy mające na celu ochronę prawa jednostki (chociażby wspomniane przyczynianie się do audytów).

Ze stosowaniem GDPR podmioty przetwarzające w Polsce dane będą się musiały zmierzyć już od wiosny 2018 r. Wydaje się jednak, że już teraz warto zacząć analizować wpływ GDPR na organizacje oraz rozpocząć proces dostosowywania obowiązujących w podmiotach rozwiązań. Proces ten może się okazać szczególnie ciężki dla organizacji, które dotąd nie zarządzały ochroną danych w sposób sprawny i świadomy.

Omni Modo
Aleja Jerzego Waszyngtona 40A, 1p.
03-910 Warszawa
NIP 113-060-77-41

tel./fax: 22 616 25 70
e-mail: omnimodo@omnimodo.com.pl
www.omnimodo.com.pl

Maciej Chodorowski

Obowiązek informacyjny w GDPR. Katalog informacji, jakie należy przekazać osobom, których dane dotyczą[8]

GDPR znacznie zmienia kształt obowiązków informacyjnych ciążących na administratorach danych osobowych. Ustawodawca unijny rozszerzył katalog informacji, jakie należy przekazać osobie, której dane dotyczą. To właśnie dzięki obowiązkom informacyjnym prawo prywatności wkracza w XXI wiek.

Pod rządami GDPR osoby, których dane dotyczą, będą posiadały wiedzę na temat tego jak dokładnie wygląda przetwarzanie ich danych osobowych. Z jednej strony większe prawa dla obywateli, a z drugiej większe obciążenia dla ADO, którzy będą musieli dokładniej uzasadniać przetwarzanie danych osobowych.

Na wstępie pragnę zaznaczyć, iż mimo wyraźnie wskazanego katalogu informacji, które powinny być udostępnione, wciąż istnieją poważne problemy interpretacyjne. Na obecną chwilę nie jesteśmy w stanie przekazać ostatecznej propozycji informacji, jakie powinny być przekazywane osobom, których dane dotyczą. Artykuł ma jednak na celu zarysowanie zakresu informacji, jakie powinny być przekazywane osobom, których dane dotyczą.

Jakie informacje należy przekazać osobom, których dane dotyczą?

Motyw 60 preambuły GDPR wskazuje nam, że osoba, której dane dotyczą, musi być poinformowana o **prowadzeniu operacji przetwarzania i o jego celach**. Poza tym administrator

[8] Artykuł pierwotnie został opublikowany pod tytułem „Jak będzie wyglądał obowiązek informacyjny w GDPR" na portalu e-ochronadanych.pl

Omni Modo
Aleja Jerzego Waszyngtona 40A, 1p.
03-910 Warszawa
NIP 113-060-77-41

tel./fax: 22 616 25 70
e-mail: omnimodo@omnimodo.com.pl
www.omnimodo.com.pl

powinien podać wszelkie inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania, uwzględniając konkretne okoliczności i kontekst przetwarzania danych osobowych.

Dodatkowo należy poinformować o fakcie **profilowania** oraz o konsekwencjach takiego profilowania. W przypadku zbierania danych od osoby, której dane dotyczą, należy wskazać, czy ma ona obowiązek je podać, oraz o konsekwencjach ich niepodania.

O czym powinniśmy poinformować zbierając dane od osoby, której dane dotyczą?

a) swojej tożsamości i danych kontaktowych oraz tożsamość i danych kontaktowych swojego przedstawiciela, jeżeli istnieje;

b) danych kontaktowych inspektora ochrony danych (jeżeli go powołaliśmy) **(nowość)**;

c) celach przetwarzania, do których mają posłużyć dane osobowe;

d) podstawie prawnej przetwarzania **(nowość);**

f) prawnie uzasadnionym interesie realizowanym przez administratora lub przez stronę trzecią – jeżeli przetwarzanie odbywa się na podstawie prawnie usprawiedliwionego interesu ADO (art. 6 ust. 1 lit. f) **(nowość);**

g) odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;

h) transferze danych do państwa trzeciego, w tym o:

- zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej **(nowość)**;
- stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony **(nowość)** lub
- wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych w przypadku przekazania danych do państwa trzeciego, o którym mowa w art. 46 , art. 47 lub art. 49 ust. 1 akapit drugi **(nowość).**

i) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu **(nowość);**

j) prawie do:

- żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą;

Omni Modo
Aleja Jerzego Waszyngtona 40A, 1p.
03-910 Warszawa
NIP 113-060-77-41

tel./fax: 22 616 25 70
e-mail: omnimodo@omnimodo.com.pl
www.omnimodo.com.pl

- ich sprostowania, usunięcia lub ograniczenia przetwarzania lub
- wniesienia sprzeciwu wobec przetwarzania, a także
- przenoszenia danych **(nowość).**

k) prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem jeżeli przetwarzanie odbywa się na podstawie zgody na przetwarzanie danych zwykłych (art. 6 ust. 1 lit. a) GDPR) lub szczególnej kategorii (art. 9 ust. 2 lit. a) GDPR) **(nowość)**;

l) prawie wniesienia skargi do organu nadzorczego **(nowość)**;

m) informacji, 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;

n) informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą **(nowość)**.

O czym powinniśmy poinformować zbierając dane z innego źródła niż osoba, której dane dotyczą?

W przypadku, gdy zbieramy dane osobowe, od innego źródła niż od osoby, której dane dotyczą zgodnie z art. 14 ust. 1 i 2 GDPR powinniśmy poinformować ją o:

a) informacjach z punktów a-l oraz n wskazanych powyżej;

b) kategoriach odnośnych danych osobowych **(nowość)**;

c) źródle pochodzenia danych osobowych, a jeżeli ma to zastosowanie, o pochodzeniu ich ze źródeł powszechnie dostępnych.

Omni Modo
Aleja Jerzego Waszyngtona 40A, 1p.
03-910 Warszawa
NIP 113-060-77-41

tel./fax: 22 616 25 70
e-mail: omnimodo@omnimodo.com.pl
www.omnimodo.com.pl

W jakiej formie mamy spełniać obowiązek informacyjny?

Powyższe informacje administrator danych powinien przekazać w **formie zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej** oraz jasnym i prostym językiem, w szczególności gdy informacje są kierowane do dziecka[9].

Klauzulę informacyjną można opatrzyć też **standardowymi znakami graficznymi**, które w widoczny, zrozumiały i czytelny sposób przedstawią sens zamierzonego przetwarzania[10].

Obowiązek informacyjny możemy spełnić **na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie**. Jednak jeżeli w treści obowiązku informacyjnego zastosowano znaki, a są one przedstawione elektronicznie, muszą nadawać się do odczytu maszynowego. Dodatkowo spełnienie obowiązku informacyjnego w stosunku do osób nie może być obarczone opłatami.

Podsumowanie

GDPR znaczenie rozszerza obowiązki informacyjne w stosunku do osób, których dane dotyczą. Administratorzy danych będą musieli przekazać podmiotom danych informacje w dużo szerszym zakresie niż to ma miejsce pod UODO. Zmiany w obowiązku informacyjnym należy uznać jako wielki przełom dla ochrony prywatności osób, których dane dotyczą. Podawanie tak szerokiego zakresu informacji, a także wysokie kary będą wymuszały dostosowanie swojej działalności do zgodności z GDPR.

Należy pamiętać o tym, że klauzule informacyjne są pierwszym miejscem, które sprawdzą inspektorzy GIODO. Ich brak zostanie natomiast uznany za ciężkie naruszenie ochrony danych osobowych (zgodnie z art. 83 ust. 5 lit. b) GDPR). W związku z czym przedmiotowe naruszenie będzie zagrożone karą do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

W obecnej chwili nie jesteśmy w stanie przewidzieć jak konkretne będą wyglądały klauzule informacyjne w dniu rozpoczęcia obowiązywania GDPR (tj. 25 maja 2018 r.). Sposób uregulowania

[9] art. 12 ust. 1 GDPR
[10] art. 12 ust. 7 GDPR

Omni Modo
Aleja Jerzego Waszyngtona 40A, 1p.
03-910 Warszawa
NIP 113-060-77-41

tel./fax: 22 616 25 70
e-mail: omnimodo@omnimodo.com.pl
www.omnimodo.com.pl

tej kwestii pojęciami otwartymi, powoduje problemy z ich obecną interpretacją. Mamy jednak nadzieję, że w ciągu dwóch następnych lat uda nam się ustalić jednolite rozumienie rozporządzenia w tej kwestii, a co za tym, ustalić dokładne informacje jakie należy przekazać osobie, której dane dotyczą by zadośćuczynić zasadom rzetelnego i przejrzystego przetwarzania danych osobowych.

Omni Modo
Aleja Jerzego Waszyngtona 40A, 1p.
03-910 Warszawa
NIP 113-060-77-41

tel./fax: 22 616 25 70
e-mail: omnimodo@omnimodo.com.pl
www.omnimodo.com.pl

Paulina Wirska

Dlaczego już teraz warto wyznaczyć inspektora ochrony danych?

Pod reżimem GDPR nieuchronnym obowiązkiem wielu przedsiębiorców będzie wyznaczenie inspektora ochrony danych (DPO). Już teraz jest ważne, aby upewnić się, że 25 maja 2018 r. Twoja firma będzie współpracować z doradcą, który weźmie na siebie odpowiedzialność za prawidłowość przetwarzania i ochrony danych osobowych.

Wiedza i profesjonalne wsparcie takiej osoby będą absolutnie niezbędne, aby spełnić skomplikowane i odmienne od krajowych wymagania unijnego prawodawcy. To od efektywności pracy DPO może zależeć, czy Twoja organizacja uniknie bardzo kosztownych konsekwencji, które przewidziano za nieprzestrzeganie GDPR.

Kto i jak będzie musiał powołać inspektora ochrony danych (DPO)?

Zgodnie z Rozporządzeniem ogólnym o ochronie danych osobowych, od 25 maja 2018 r. obowiązkiem wielu przedsiębiorców będzie wyznaczenie inspektora ochrony danych (DPO).

Artykuł 37 GDPR stanowi, że jesteś zobowiązany do wyznaczenia inspektora ochrony danych w firmie, jeśli:

- 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,

Omni Modo
Aleja Jerzego Waszyngtona 40A, 1p.
03-910 Warszawa
NIP 113-060-77-41

tel./fax: 22 616 25 70
e-mail: omnimodo@omnimodo.com.pl
www.omnimodo.com.pl

- główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych (danych wrażliwych).

ABI i DPO – to jest to samo?

Istnieją pewne podobieństwa, ale różnice również są wyraźne.

Obecnie obowiązująca Ustawa o ochronie danych osobowych w rozdziale „Zabezpieczenie danych" stanowi, że administrator danych może powołać administratora bezpieczeństwa informacji, do którego zadań będzie należało m.in. zapewnianie przestrzegania przepisów o ochronie danych osobowych. Jest to jednak uprawnienie a nie obowiązek.

Jeżeli w twojej firmie został wyznaczony ABI to na pewno pomoże łagodnie przeprowadzić całą organizację przez skomplikowany proces dostosowywania do wymogów GDPR.

Co stanowi GDPR w sprawie zadań, pozycji i wymagań wobec DPO?

GDPR określa minimalne zadania DPO. Ponadto wprowadza wyjaśnienia w sprawie stanowiska DPO w ramach organizacji, takich jak jego/jej linii raportowania, w jaki sposób praca musi być wykonana i obowiązków administratora danych w celu umożliwienia tej pracy.

Do zadań DPO należeć będzie:

1. informowanie i doradzanie pracownikom – którzy przetwarzają dane osobowe – o obowiązkach DPO, obowiązkach wynikających z GDPR i innych przepisów UE lub lokalnych w zakresie ochrony danych;
2. monitorowanie zgodności z GDPR, z innymi przepisami dotyczącymi ochrony danych (lokalnymi i UE) lub z zasadami ochrony danych obowiązującymi w organizacji, włącznie z przypisaniem odpowiedzialności, podnoszenie świadomości i szkolenia personelu uczestniczącego w procesach przetwarzania danych, a także prowadzenie związanych z nimi kontroli;
3. dostarczanie administratorowi danych niezbędnych informacji i monitorowanie działań pod kątem oceny skutków – „data protection impact assessment"
4. monitorowanie i zgłaszanie w trybie przewidzianym w artykule 33 i 34 GDPR albo informowanie w inny sposób GIODO i osób, których dane dotyczą o przypadkach

Omni Modo
Aleja Jerzego Waszyngtona 40A, 1p.
03-910 Warszawa
NIP 113-060-77-41

tel./fax: 22 616 25 70
e-mail: omnimodo@omnimodo.com.pl
www.omnimodo.com.pl

naruszenia ochrony danych osobowych. Rolą DPO jest też dokumentowanie wniosków osób, których dane dotyczą oraz organów publicznych w zakresie usuwania, niszczenia lub udostępniania danych;

5. działanie jako punkt kontaktowy organizacji w kwestiach związanych z przetwarzaniem danych osobowych, w tym wcześniejszą konsultacją;
6. przygotowywanie odpowiedzi do osób, których dane są przetwarzane (pracowników, klientów i innych osób) we wszystkich kwestiach związanych z przetwarzaniem ich danych i wykonywaniem ich praw wynikających z GDPR.

Kto może być DPO?

Musisz wyznaczyć DPO na podstawie stopnia profesjonalizmu kandydata, a w szczególności, eksperckiego poziomu znajomość prawa i praktyki w zakresie ochrony danych oraz zdolności do wypełniania zadań wymienionych powyżej.

W każdym procesie rekrutacji idealne wymagania są połączeniem twardych umiejętności (np. wiedza, doświadczenie zawodowe i znajomość języków) i miękkich umiejętności (przywództwo, komunikacja, negocjacje), które razem tworzą zestaw cech potrzebnych, aby wykonać zadanie.

Wybór DPO musi być decyzją dobrze przemyślaną. Inspektor musi posiadać doświadczenie zawodowe i wiedzę specjalistyczną w dziedzinie ochrony danych, w tym głębokie zrozumienie rozporządzenia o ochronie danych UE (GDPR). Wymagany poziom wiedzy nie jest ściśle określony, ale oczywiście powinien być współmierny do charakteru i zakresu danych, „rozmachu" procesów przetwarzania danych a także samej wielkości organizacji przedsiębiorcy.

Jak ocenić „odpowiedni" poziom wiedzy, jakiego powinniśmy oczekiwać od naszego inspektora?

Rozporządzenie wzywa nas do poszukiwania "eksperta". Jednak to do nas należy określenie poziomu wiedzy w stosunku do naszego rodzaju przetwarzania i wymaganego poziomu ochrony. Oznaczałoby to, że firmy, które cechuje większe ryzyko (ponieważ bazują na danych lub przetwarzają dane wrażliwe lub też w dużym stopniu polegają na outsourcingu) muszą szukać kogoś, kto ma wysoki poziom wiedzy fachowej w dziedzinie prawa i praktykę w jego stosowaniu.

Omni Modo
Aleja Jerzego Waszyngtona 40A, 1p.
03-910 Warszawa
NIP 113-060-77-41

tel./fax: 22 616 25 70
e-mail: omnimodo@omnimodo.com.pl
www.omnimodo.com.pl

Z drugiej strony, jeśli przetwarzanie jest ograniczone w rodzaju, skali i geografii, to może być wystarczające, aby zatrudnić kogoś, kto ma niższy poziom wiedzy.

Kolejna na liście jest "zdolność do wypełniania zadań". Jakie umiejętności mogą umożliwić spełnienie wszystkich wymienionych zadań? Oczywiście, nasza znajomość dziedziny i poprzednie podobne doświadczenia zdecydowanie zwiększają tą zdolność. Jednakże, istnieją jeszcze inne cechy, które są równie ważne, aby dobrze wykonać pracę. Szukamy profesjonalistów z doskonałymi umiejętnościami interpersonalnymi na wszystkich poziomach organizacji, kogoś, kto jest w stanie pracować w sposób uporządkowany i pod minimalnym nadzorem, umie ocenić ryzyko. Również logiczne wydaje się, że DPO powinien wyróżniać się umiejętnościami komunikacyjnymi, ponieważ do pełnienia tej funkcji nie jest wystarczająca sama znajomość przepisów – DPO musi również być zdolny do efektywnego i wiarygodnego dzielenia się swoją wiedzą. Dodatkowo, DPO musi być zorientowany w sztuce zarządzania zmianą, aby móc biegle stosować swoją wiedzę do opracowywania i wdrażania konkretnej praktyki ochrony danych.

Czy na DPO można powołać pracownika?

Konstrukcja przepisu jednoznacznie wskazuje na możliwość outsourcingu świadczonego przez wyspecjalizowane w tym podmioty. Jednak DPO może być też członek personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług. W takim wypadku trzeba bezwzględnie zapewnić, aby pozostałe obowiązki służbowe współgrały z nowymi obowiązkami jako DPO i nie spowodowały konfliktu interesów.

Czy firmy mogą mieć wspólnego in-house DPO?

GDPR wprost wskazuje na możliwość pełnienia funkcji DPO przez jedną osobę dla całej grupy przedsiębiorstw. Konieczne jest jednak zapewnienie łatwego dostępu do inspektora przez każdy z podmiotów. Dodatkowo należy pamiętać, że taki wspólny wewnętrzny DPO musi w równym stopniu wypełniać swoje obowiązki wobec wszystkich zarządów, pracowników spółek oraz organów nadzorczych.

Omni Modo
Aleja Jerzego Waszyngtona 40A, 1p.
03-910 Warszawa
NIP 113-060-77-41

tel./fax: 22 616 25 70
e-mail: omnimodo@omnimodo.com.pl
www.omnimodo.com.pl

Komu podlega DPO organizacyjnie?

Zgodnie z GDPR inspektor ochrony danych będzie raportował bezpośrednio zarządowi organizacji. DPO musi zajmować pozycję pozwalającą na wykonywanie zadań wynikających z GDPR w sposób niezależny. Dlatego DPO nie może przyjmować instrukcji odnośnie swoich zadań ani nie może być zagrożony konsekwencjami dyscyplinarnymi za ich wykonywanie (np. współpracę z organem nadzorczym).

Wyrażenie "żadnych instrukcji" w rozporządzeniu odnosi się do niezależności operacyjnej przy realizacji kluczowych zadań. Jako ekspert inspektor ochrony danych wspiera organizację w celu osiągnięcia celów biznesowych w sposób zgodny z zasadami ochrony danych osobowych. Dlatego musi być w stanie udzielać porad swobodnie; decyzja o tym, czy iść za radą eksperta ostatecznie spoczywa na firmie.

Obowiązki pracodawcy wobec DPO

Administrator danych musi:

1. wspierać swojego DPO poprzez zapewnienie zasobów niezbędnych do wykonywania jego/jej zadań, a także w celu utrzymania jego/jej wiedzy eksperckiej;
2. zapewnić dostęp do danych osobowych i procesów przetwarzania danych;
3. upewniać się, że inspektor jest prawidłowo i terminowo zaangażowany we wszystkie sprawy, które odnoszą się do ochrony danych osobowych;
4. udostępnić dane kontaktowe DPO organowi nadzorczemu oraz opinii publicznej.

Co do "zasobów", są to rzeczy takie jak dodatkowy personel, budżet specjalistycznych narzędzi, które mogą umożliwić lepszą wydajność, np. oprogramowanie. Wspieranie utrzymania wiedzy DPO to zapewnienie specjalistycznych kursów prowadzonych przez instytucje publiczne lub prywatne, programy certyfikacyjne, seminaria, konferencje, książki itp.

Upewnianie się, że inspektor jest prawidłowo i terminowo zaangażowany we wszystkie sprawy to w szczególności "dobra wola" zarządu, aby traktować DPO nie jak przedłużone ramię regulatora – GIODO, ale raczej jako zaufanego doradcę, który pomaga firmie osiągnąć cele.

Omni Modo
Aleja Jerzego Waszyngtona 40A, 1p.
03-910 Warszawa
NIP 113-060-77-41

tel./fax: 22 616 25 70
e-mail: omnimodo@omnimodo.com.pl
www.omnimodo.com.pl

Konsekwencje braku DPO

Jak widać powyżej, zatrudnienie DPO to dużo dodatkowych wymagań dla administratora. Czy w takim razie można „pominąć" ten jeden przepis GDPR? Odpowiedź w formie wskazówki: naruszenie GDPR polegające na niewyznaczeniu DPO tam, gdzie wymaga tego regulacja może spowodować wysokie grzywny administracyjne (do 10 000 000 EUR, albo nawet do 2% całkowitej światowej rocznego obrotu w poprzednim roku obrotowym).

Czy leci z nami ABI?

Obecnie obowiązująca UODO w rozdziale „Zabezpieczenie danych" stanowi, że administrator danych może powołać administratora bezpieczeństwa informacji, do którego zadań będzie należało m.in. zapewnianie przestrzegania przepisów o ochronie danych osobowych.

Dlatego, właśnie teraz jest najlepsza pora na spokojne zastanowienie się, czy obecne podejście Twojej firmy do ochrony danych osobowych zapewni łagodne wejście w nowy porządek prawny w zakresie ochrony danych osobowych.

Jeżeli Twoja firma jest wspierana przez rozsądnego ABI to najpewniej osoba ta już od wielu miesięcy intensywnie pracuje nad zapewnieniem zgodności z prawem procesów przetwarzania danych w 2018 r. Tylko taką osobę, gotową na podjęcie wszystkich wyzwać GDPR, warto wyznaczyć na DPO.

Omni Modo
Aleja Jerzego Waszyngtona 40A, 1p.
03-910 Warszawa
NIP 113-060-77-41

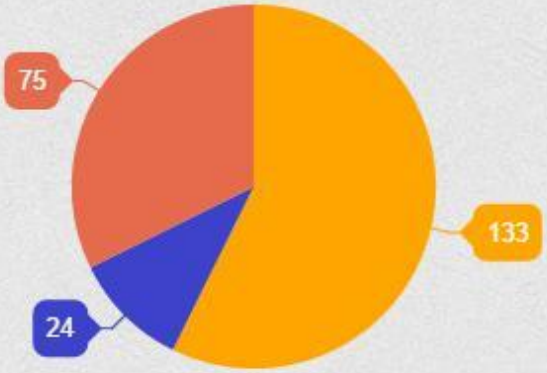
tel./fax: 22 616 25 70
e-mail: omnimodo@omnimodo.com.pl
www.omnimodo.com.pl

Podsumowanie ankiety o unijnym rozporządzeniu o ochronie danych osobowych (GDPR/RODO)

NA NASZE PYTANIA ODPOWIEDZIAŁY 233 OSOBY

W ankiecie brali udział:

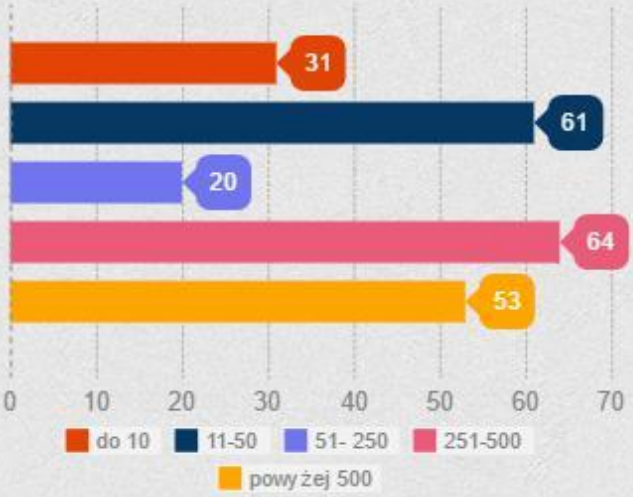
- ABI(57.33%)
- Osoby zarządzające(10.34%)
- Pracownicy(32.33%)



W jakiej branży działają organizacje ankietowanych?

Administracja publiczna(34.05%) Motoryzacja(0.86%) Doradztwo prawne/ konsulting(11.21%) E-commerce(2.16%)
Finansowa/ Bankowość"(7.33%) Handel/ Usługi(5.60%) HR(0.86%) IT/ Technologiczna(10.34%)
Kreatywna/ Marketing(5.60%) NGO(1.29%) Ochrona zdrowia(5.60%) Przemysł/Budownictwo(6.03%)
Spółdzielcza(3.02%) Szkolnictwo(3.45%) Telekomunikacja(2.59%)

Wielkość organizacji respondentów?



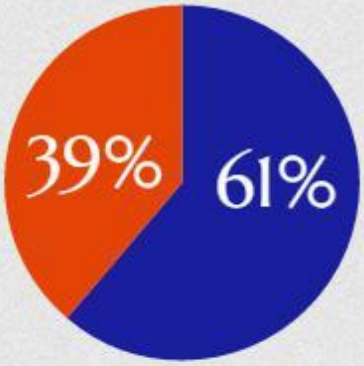
W naszym badaniu wzięły udział głównie osoby zatrudnione w dużych i bardzo dużych organizacjach. Może oznaczać to, iż to właśnie od wielkości organizacji zależy jak wcześnie rozpoczyna się przygotowania GDPR/RODO. Należy pamiętać o tym, że im większa organizacja tym potrzeba więcej czasu na dostosowanie jej funkcjonowania do rozporządzenia.

25%

ABI rozpoczęło już przygotowania do GDPR/RODO

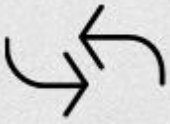
Ponad 1/4 ankietowanych ABI zadeklarowała, że rozpoczęła już przygotowania do rozporządzenia. Wynik ten w porównaniu z grupą ankietowanych wskazuje na to, iż ABI w większych podmiotach mają świadomość tego, że wdrożenie zmian może zająć im więcej czasu.

Ile osób wiedziało od kiedy zaczną obowiązywać przepisy GDPR/RODO?

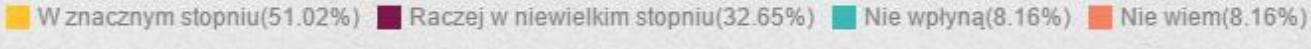


Ponad 2/3 Ankietowanych odpowiedziało poprawnie na pytanie o rozpoczęcie obowiązywania przez GDPR/RODO. Tak dobry wynik możemy przypisać szeroko zakrojonej kampanii edukacyjnej prowadzonej przez organy Państwowe oraz firmy prywatne.

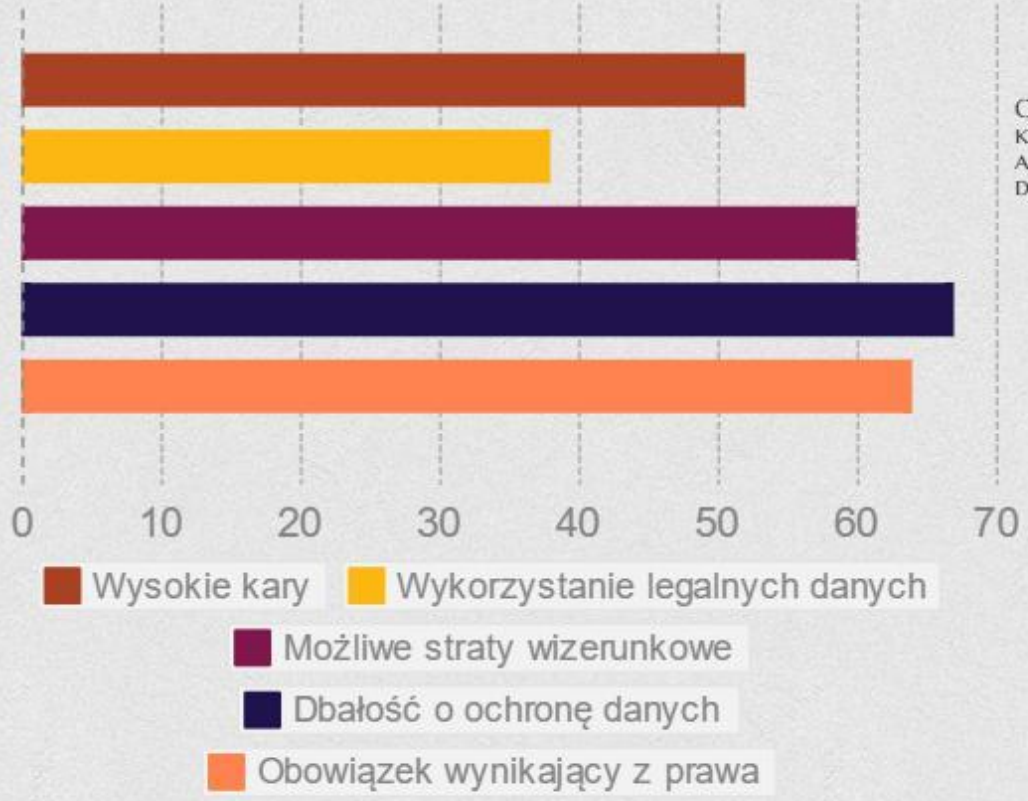
Czy nowe unijne przepisy wpłyną na prowadzoną działalność gospodarczą?



Według ok. 80% Ankietowanych nowe przepisy będą miały wpływ na ich działalność. Taki wynik możemy uzasadnić dużymi zmianami jakie wprowadzi w systemie ochrony danych nowe rozporządzenie.

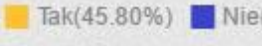


Co skłania ankietowanych do przestrzegania nowych przepisów GDPR/RODO?



Okazuje się, że to nie wysokie kary najbardziej motywują ankietowanych do ochrony danych osobowych.

Czy osoby zarządzające zamierzają zwiększyć zasoby personalne lub finansowe na ochronę danych osobowych?



Prawie połowa osób zarządzających wskazała, iż zamierza zwiększyć nakłady finansowe na ochronę danych osobowych. W związku z dużymi zmianami jakie Organizacje będą musiały przeprowadzić niezbędne wydaje się zwiększenie środków do ochrony danych osobowych.

82%

osób zarządzających zamierza korzystać z doświadczenia firm zewnętrznych w związku z wdrożeniem GDPR/RODO

Czy pracownicy obawiają się zwiększenia ich obowiązków służbowych w związku z obowiązywaniem GDPR/RODO?

Autorzy

Marcin Cwener
tel.: +48 690 380 382 e-mail: m.cwener@omnimodo.com.pl

Prawnik, absolwent Wydziału Prawa i Administracji Uniwersytetu Szczecińskiego oraz studiów podyplomowych na kierunku „Zarządzanie Bezpieczeństwem Informacji" w Szkole Głównej Handlowej w Warszawie. W latach 2012-2013 pracownik Departamentu Orzecznictwa, Legislacji i Skarg w Biurze Generalnego Inspektora Ochrony Danych Osobowych, gdzie zajmował się prowadzeniem postępowań administracyjnych. W Omni Modo prowadzi audyty i szkolenia, a także pełni funkcję zewnętrznego Administratora Bezpieczeństwa Informacji. Do jego szczególnych zainteresowań należy kwestia powiązań ustawy o ochronie danych osobowych z prawem bankowym oraz kanonicznym.

Marta Bargiel- Kaflik
tel.: +48 506 073 117 e-mail: m.bargiel@omnimodo.com.pl

Prawnik, absolwentka Wydziału Prawa i Administracji Uniwersytetu Marii Curie – Skłodowskiej w Lublinie oraz studiów podyplomowych na kierunku „Zarządzanie Bezpieczeństwem Informacji" w Szkole Głównej Handlowej w Warszawie. Ukończyła Suffolk County Community College (NY) oraz Long Island University (NY). Wieloletni pracownik Departamentu Orzecznictwa, Legislacji i Skarg w Biurze Generalnego Inspektora Ochrony Danych Osobowych, prowadzący postępowania administracyjne o wysokim stopniu skomplikowania. Specjalizuje się w prawie pracy i przetwarzaniu danych w związku z procesami rekrutacyjnymi i zatrudnianiem pracowników.

Omni Modo
Aleja Jerzego Waszyngtona 40A, 1p.
03-910 Warszawa
NIP 113-060-77-41

tel./fax: 22 616 25 70
e-mail: omnimodo@omnimodo.com.pl
www.omnimodo.com.pl

Maciej Chodorowski
tel.: +48 508 388 242 e-mail: m.chodorowski@omnimodo.com.pl

Prawnik, absolwent Wydziału Prawa i Administracji Uniwersytetu Marii Curie – Skłodowskiej w Lublinie. Doświadczenie zawodowe zdobywał w firmach konsultingowych zajmujących się bezpieczeństwem informacji. Maciek specjalizuje w przetwarzaniu danych osobowych w marketingu internetowym oraz w problematyce powiązań danych osobowych z tajemnicą przedsiębiorstwa. W Omni Modo obsługuje podmioty z szeroko pojętej branży produkcyjnej, e-commerce oraz kreatywnej.

Paulina Wirska
tel.: +48 503 326 582 e-mail: p.wirska@omnimodo.com.pl

Prawnik z doświadczeniem w zakresie ochrony danych osobowych. Absolwentka Kolegium Prawa w Akademii Leona Koźmińskiego w Warszawie. Doświadczenie zawodowe zdobywała jako wieloletni pracownik Departamentu Orzecznictwa Legislacji i Skarg w Biurze Generalnego Inspektora Ochrony Danych Osobowych, Departamencie Spraw Obywatelskich Ministerstwa Spraw Wewnętrznych i Administracji oraz Departamencie Prawnym Ministerstwa Cyfryzacji. Prowadzi audyty i szkolenia, doradza administratorom danych osobowych. Współtworzy także serwis e-ochronadanych.pl. Interesuje się prawem nowych technologii, a także kulturą i literaturą iberoamerykańską.

Omni Modo
Aleja Jerzego Waszyngtona 40A, 1p.
03-910 Warszawa
NIP 113-060-77-41

tel./fax: 22 616 25 70
e-mail: omnimodo@omnimodo.com.pl
www.omnimodo.com.pl

O nas

Omni Modo to po łacinie „na każdy sposób". Nazwa naszej firmy to nie przypadek. Na każdy sposób bowiem chcemy pokazywać klientom nasze doświadczenie, profesjonalizm i sukcesy w dziedzinie ochrony danych osobowych.

Doświadczenie to: historia naszej firmy

Tworzymy ją nieprzerwanie od 12 lat stale dostosowując ofertę do potrzeb rynku. Swoimi działaniami wspieramy zarówno małe firmy, jak i korporacje, czy organy administracji. Współtworzymy również pierwszy w Polsce portal dotyczący ochrony danych osobowych www.e-ochronadanych.pl.

Doświadczenie i profesjonalizm to: nasz zespół

Udało nam się zebrać grono ekspertów w dziedzinie ochrony danych osobowych: radców prawnych, adwokatów, byłych pracowników departamentów prawnych Biura GIODO oraz specjalistów ds. bezpieczeństwa w branży IT. Nasi specjaliści są współautorami książek (m.in. „Ochrona danych osobowych – wybór zagadnień") oraz licznych artykułów i opracowań w tej dziedzinie. Każdy z nich to zawodowa indywidualność, łączy ich jedno: duża branżowa wiedza i stale podnoszone kwalifikacje.

Doświadczenie, profesjonalizm i sukcesy to: liczby

Jako jedni z pierwszych zaoferowaliśmy usługę zewnętrznego Administratora Bezpieczeństwa Informacji, z której do chwili obecnej skorzystało ponad 70 firm. Ponadto, doradzaliśmy w kwestiach związanych z ochroną danych osobowych kilkuset podmiotom z różnych branż. Zorganizowaliśmy szereg szkoleń otwartych i zamkniętych, w trakcie których przeszkoliliśmy kilkanaście tysięcy osób (średnio 1500 rocznie). Przeprowadzamy również kilkadziesiąt audytów rocznie.

Omni Modo
Aleja Jerzego Waszyngtona 40A, 1p.
03-910 Warszawa
NIP 113-060-77-41

tel./fax: 22 616 25 70
e-mail: omnimodo@omnimodo.com.pl
www.omnimodo.com.pl