FORSAFE

BEZPIECZEŃSTWO PONAD WSZYSTKO

RODO

najważniejsze zmiany i nowości

Praktyczny zestaw pytań i odpowiedzi na zagadnienia związane z europejskim rozporządzeniem w sprawie ochrony danych osobowych

Spis treści

1. Co to jest RODO?

Pod pojęciem „RODO lub GDPR" kryje się **rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych** oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). Jest to akt prawny przyjęty przez Unię Europejską regulujący zasady ochrony danych osobowych – zastępuje dyrektywę 95/46/WE z 1995 r. Przepisy RODO mają zastosowanie bezpośrednio od 25 maja 2018r. Uzupełnieniem jest Polska Ustawa o Ochronie Danych Osobowych z dnia 10.05.2018 Dz. U. z 2018 r., poz. 1000.

2. Jaka jest historia regulacji o ochronie danych osobowych?

Historia regulacji dotyczących przepisów o ochronie danych osobowych ma już 20 lat. Za jej początek przyjmujemy uchwalenie dyrektywy 95/46/WE – podstawowego aktu prawnego regulującego zasady ochrony danych osobowych w całej Europie. 4 listopada 2010 r. Komisja Europejska opublikowała komunikat zatytułowany „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej". 25 stycznia 2012 r. Komisja Europejska przedstawiła opis najważniejszych elementów reformy ochrony danych. Ich założenia zostały wprowadzone w życie pod koniec 2015 r.

Po przyjęciu przez Radę dokumentów, w kwietniu 2016r. Parlament przegłosował pakiet nowych unijnych ram prawnych dla ochrony danych osobowych, czyli RODO. Równocześnie z wejściem w życie europejskiego rozporządzenia od dn. 25.05.2018 obowiązuje Polska Ustawa o Ochronie Danych Osobowych.

24.10.1995
Uchwalenie dyrektywy 95/46/WE

29.08.1997
Polska ustawa o ochronie danych osobowych

4.11.2010
Całościowe podejście do kwestii ochrony danych osobowych w EU.

25.01.2012
KE przedstawiła opis elementów reformy ochrony danych – ich założenia zostały wprowadzone w życie pod koniec 2015 r.

27.04.2016
Uchwalenie RODO

10.05.2018
Nowa polska ustawa o ochronie danych osobowych

25.05.2018
Obowiązywanie RODO

3. Jaki jest cel i zastosowanie RODO?

Głównym celem RODO jest potwierdzenie faktu, że ochrona danych osobowych jest podstawowym prawem każdego obywatela. Rozporządzenie wprowadza szereg uprawnień dla osób prywatnych oraz obowiązków dla przedsiębiorców i instytucji przetwarzających dane osobowe.

4. Kto podlega RODO? Kto powinien wdrożyć RODO?

RODO podlega każdy przedsiębiorca/instytucja, prowadząca działalność na terenie Unii Europejskiej. Może to być działalność w jakiejkolwiek formie prawnej: spółka, jednoosobowa działalność gospodarcza, czy nawet oddział w Unii Europejskiej przedsiębiorcy mającego siedzibę poza Unią. Nie ma znaczenia narodowość osób, których dane osobowe są przetwarzane.

RODO stosujemy, gdy:

a. przetwarzanie danych osobowych odbywa się w związku z działalnością prowadzoną przez jednostkę organizacyjną[1] Administratora lub podmiotu przetwarzającego w Unii

b. przetwarzanie danych osobowych osób fizycznych przebywających w Unii odbywa się przez Administratora lub podmiot przetwarzający, niemającego jednostek organizacyjnych w Unii, jeżeli czynności przetwarzania wiążą się z:

- oferowaniem towarów lub usług takim osobom, których dane dotyczą, w Unii – niezależnie od tego, czy wymaga się od tych osób zapłaty;

lub

- monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii[2].

c. przetwarzanie danych osobowych odbywa się przez Administratora niemającego jednostki organizacyjnej w Unii, ale posiadającego jednostkę organizacyjną w miejscu, w którym na mocy prawa międzynarodowego publicznego ma zastosowanie prawo państwa członkowskiego.

Ochrona danych osobowych nie znajduje zastosowania do działalności osobistej lub domowej. To oznacza, że osoba fizyczna prowadząca działalność gospodarczą musi stosować RODO do przetwarzania danych osobowych wyłącznie swoich klientów czy pracowników.

Rozporządzenie nie ma również zastosowania do przetwarzania danych osobowych w ramach działalności nieobjętej zakresem prawa Unii (np. kwestie związane z bezpieczeństwem narodowym), a także do działalności związanej z przetwarzaniem danych przez instytucje unijne czy też dyplomatyczne. Przepisów rozporządzenia nie stosuje się również do działalności właściwych organów w celu zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

---

[1] Jednostka organizacyjna oznacza prowadzenie działalności poprzez stabilne struktury, np. oddział, spółka zależna.

[2] Monitorowanie zachowania oznacza obserwowanie osoby fizycznej w Internecie, polegające na dokonaniu profilowania w celu podjęcia decyzji jej dotyczącej lub przeanalizowania bądź prognozowania jej osobistych preferencji, zachowań i postaw.

5. Co to są dane osobowe?

Dane osobowe to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Taką osobę można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora, takiego jak:

imię i nazwisko, adres zamieszkania

numer PESEL, seria i numer dokumentu tożsamości

numer telefonu, adres e-mail, wizerunek

Wyróżnia się dwie kategorie danych osobowych:

a) tzw. dane osobowe zwykłe,

b) dane osobowe zaliczające się do szczególnych kategorii danych (dawniej zwane danymi wrażliwymi).

Do szczególnych kategorii danych osobowych zaliczamy dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej. Dane osobowe, które nie należą do żadnej z tych kategorii, to dane zwykłe.

Dane osobowe szczególnej kategorii:

- **Dane genetyczne** - dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej.
- **Dane biometryczne** - wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.
- **Dane dotyczące zdrowia** - dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia.

Przetwarzania danych osobowych dotyczących wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa na podstawie art. 6 ust. 1 wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. Wszelkie kompletne rejestry wyroków skazujących są prowadzone wyłącznie pod nadzorem władz publicznych

6. Co to jest przetwarzanie danych osobowych w rozumieniu RODO?

RODO stosuje się do operacji przetwarzania danych osobowych.
Przetwarzaniem danych osobowych są jakiekolwiek operacje wykonywane na danych osobowych, takie jak:

Co bardzo ważne, RODO obejmuje wszelkie czynności, których przedmiotem są dane osobowe – czyli nie tylko np. usługę archiwizowania dokumentów, ale wszelkie usługi począwszy od zbierania do archiwizacji i usunięcia włącznie z czynnościami wykonywanymi w systemach informatycznych.

7. Kto przetwarza dane osobowe?

Przetwarzanie danych osobowych, może być wykonywane przez:

- Administratora danych,
- podmiot przetwarzający dane,
- inne podmioty przetwarzające dane,
- osoby upoważnione do przetwarzania danych.

Rola, jaką pełni Administrator danych jest kluczowa z punktu widzenia obowiązków oraz praw osób fizycznych.

Administratorem danych nazywamy podmiot decydujący o celach i sposobach przetwarzania danych. Będzie to np.:

- pracodawca w stosunku do swoich pracowników,
- sprzedawca w sklepie internetowym w stosunku do swoich klientów,
- właściciel strony internetowej w stosunku do subskrybentów newsletteru.

Administratorem danych jest zawsze określony podmiot, np. spółka, a nie jego pracownik. Przykłady:

- Administratorem danych jest spółka z o.o., a nie jej prezes zarządu, czy dyrektor marketingu,
- Administratorem jest Jan Kowalski prowadzący działalność gospodarczą.

Obowiązki Administratora danych:

- uwzględnianie ochrony danych w fazie projektowania oraz zapewnienie domyślnej ochrony danych,
- rejestrowanie czynności przetwarzania danych,
- zapewnienie bezpieczeństwa przetwarzania,
- zawieranie umów powierzenia przetwarzania danych osobowych,
- zgłaszanie naruszeń ochrony danych,
- zawiadamianie osób, których dane dotyczą o naruszeniach,
- ocena skutków dla ochrony danych,
- szacowanie ryzyka,
- zapewnienie zgodności przetwarzania z RODO.

Podmiot przetwarzający dane osobowe nie decyduje o celach i środkach przetwarzania danych – działa na podstawie umowy z Administratorem danych. Administrator danych może bowiem albo sam przetwarzać dane, albo skorzystać z usług zewnętrznego podmiotu, który te dane będzie przetwarzał dla niego. Przykłady:

- biuro rachunkowe przetwarza na zlecenie dane osobowe przekazane w tym celu przez klientów,
- podmiot odpowiedzialny za utrzymanie systemu informatycznego Administratora,
- podmiot zajmujący się niszczeniem danych osobowych.

Administrator danych powierzając czynności przetwarzania danych jest zobowiązany zawrzeć z podmiotem przetwarzającym danych odpowiednią umowę, tzw. umowę powierzenia, w której określone zostaną zasady przetwarzania danych.

W każdej organizacji dane osobowe przetwarzają konkretne osoby fizyczne – pracownicy lub współpracownicy Administratora lub podmiotu przetwarzającego dane. Takie osoby powinny posiadać upoważnienie do przetwarzania danych osobowych.

8. Status i obowiązki inspektora ochrony danych osobowych

RODO wprowadza nową definicję osoby odpowiedzialnej za nadzór nad ochroną danych osobowych. Jest nią **Inspektor ochrony danych osobowych (wcześniej Administrator Bezpieczeństwa Informacji).** Wyznaczany jest on przez Administratora danych w celu wspomagania oraz nadzorowania systemu ochrony danych osobowych.

Inspektor ochrony danych może być członkiem personelu Administratora danych lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług. Administrator danych lub podmiot przetwarzający publikują dane kontaktowe Inspektora ochrony danych i zawiadamiają o nich organ nadzorczy.

Inspektor ochrony danych osobowych jest odpowiedzialny za:

- informowanie Administratora danych oraz pracowników o obowiązkach,
- monitorowanie przestrzegania rozporządzenia,
- szkolenia personelu uczestniczącego w operacjach przetwarzania,
- audyty,
- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych,
- współpraca z organem nadzorczym,
- pełnienie funkcji punktu kontaktowego dla organu nadzorczego.

Ogólne rozporządzenie o ochronie danych (RODO) w art. 37 ust 1 przewiduje obowiązek wyznaczenia inspektora dla Administratorów i podmiotów przetwarzających wówczas, gdy:

a. przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
b. 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.
c. główna działalność Administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o których mowa w art. 10.

Ponadto zgodnie z art. 37 ust. 4 ogólnego rozporządzenia o ochronie danych obowiązek powołania inspektora ochrony danych może wprowadzić prawo Unii lub prawo państwa członkowskiego. Oznacza to, iż m.in. ustawodawca polski będzie mógł rozszerzyć obowiązek wyznaczenia IOD na inne podmioty. W pozostałych przypadkach wyznaczenie inspektora będzie fakultatywne i powinno być określane indywidualnie.

9. Zasady zbierania i przetwarzania danych osobowych

Dane osobowe można przetwarzać wyłącznie wtedy, gdy istnieje tzw. **przesłanka legalizująca przetwarzanie danych osobowych**. Dane osobowe możemy przetwarzać, gdy:

- posiadamy zgodę na przetwarzanie swoich danych osobowych,
- wykorzystujemy je w celu wykonania lub przygotowania umowy,
- jest to niezbędne do wypełnienia obowiązku prawnego,
- jest to niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą,
- jest to niezbędne do wykonania zadania realizowanego w interesie publicznym,
- jest to niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora Danych.

W przypadku szczególnych kategorii danych, typowe podstawy przetwarzania danych to:

a. wyraźna zgoda osoby, której dane dotyczą,
b. przetwarzanie danych jest niezbędne do wykonania zadań związanych z zatrudnieniem, ubezpieczeniem społecznym pracowników,
c. przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy,
d. przetwarzanie danych jest niezbędne w celu dochodzenia praw przed sądem.

To Administrator danych powinien móc wykazać, że dysponuje odpowiednią podstawą przetwarzania danych. Fakt ten wynika z tzw. zasady rozliczalności zawarta w art. 6 i 9 RODO. Każda zgoda na przetwarzanie danych powinna charakteryzować się następującymi cechami:

a. **dobrowolność** – zgoda może być ważna tylko jeżeli osoba, której dane dotyczą, ma możliwość dokonania rzeczywistego wyboru, przy czym nie zachodzi ryzyko wprowadzenia w błąd, zastraszenia, przymusu lub znaczących negatywnych konsekwencji, jeśli nie wyrazi zgody. Jeżeli konsekwencje wyrażenia zgody nie dają się pogodzić ze swobodą wyboru, zgoda nie jest dobrowolna,
b. **konkretność** – aby zgoda była ważna, musi być konkretna. Innymi słowy, niedopuszczalna jest ogólna zgoda bez określenia dokładnego celu przetwarzania,
c. **świadomość** – zgoda na przetwarzanie danych osobowych nie może mieć charakteru abstrakcyjnego, lecz winna odnosić się do skonkretyzowanego stanu faktycznego, obejmując tylko określone dane oraz sprecyzowany sposób i cel ich przetwarzania,
d. **jednoznaczność** – zgoda musi mieć charakter wyraźny, a jej wszystkie aspekty muszą być jasne dla podpisującego w momencie jej wyrażania.

Zgoda może zostać wyrażona w dowolnej formie – ale zawsze w razie wątpliwości to Administrator danych powinien wykazać, że zgoda została udzielona. Decyzja o tym, jaki konkretnie sposób zbierania – i archiwizowania – zgód zastosować powinna być podjęta świadomie przez Administratora danych.

Przetwarzanie danych osobowych jest możliwe w oparciu o poniższe zasady:

Zasada zgodności z prawem, rzetelności i przejrzystości
Dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą.

Zasada ograniczenia celu
Dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.

Zasada minimalizacji danych
Dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

Zasada prawidłowości
Dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane.

Zasada ograniczenia przechowywania
Dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.

Zasada integralności i poufności
Dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

Zgodę na przetwarzanie danych osobowych można zawsze odwołać i powinno być to równie łatwe jak jej udzielenie. Oznacza to, że w przyszłości nie można się już opierać na takiej cofniętej zgodzie, jednak nie dotyczy to czynności, które miały miejsce w przeszłości.

10. Obowiązek informacyjny

Obowiązek informacyjny to nic innego, jak udzielenie osobie, której dane dotyczą informacji o zasadach przetwarzania jej danych oraz o tym, jakie prawa jej przysługują. Informacje te są przekazywane podczas zbierania danych, a także wtedy, gdy są uzyskiwane od innego podmiotu (np. podczas zakupu legalnej bazy marketingowej). Informacji udziela ten kto otrzymał dane. W przypadku bezpośredniego pozyskania danych, jeżeli te informacje są już znane osobie, której dane dotyczą, nie ma obowiązku udzielania niezbędnych informacji (Art. 13 ust. 4 RODO), np. w przypadku zawarcia umowy z tą osobą, uzasadnione jest stwierdzenie, że ma ona już wiedzę o przetwarzaniu jej danych, gdy wynika ono bezpośrednio z celu zawarcia umowy.

Obowiązek informacyjny powinien zawierać:

- informację o tożsamości Administratora danych i o jego danych kontaktowych,
- jeżeli Administrator danych powołał Inspektora Ochrony Danych (IOD) – o danych kontaktowych IOD,
- jasne wskazanie celów i podstawie przetwarzania danych,
- informację o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją
- gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego,
- dane o okresie czasu, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
- informację o prawie do żądania od Administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
- jeżeli przetwarzanie odbywa się na podstawie zgody – informację o prawie do cofnięcia zgody w dowolnym momencie,
- informację o prawie wniesienia skargi do organu nadzorczego,
- jeżeli dochodzi do tzw. zautomatyzowanego podejmowania decyzji lub profilowania – należy poinformować tym fakcie oraz podać istotne informacje o zasadach automatycznego podejmowania decyzji, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania.

Przykładowy obowiązek informacyjny może wyglądać jak poniżej:

Obowiązek Informacyjny

Działając zgodnie z art. 13 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.U.UE.L.2016.119.1), dalej jako: „RODO" informujemy, iż:

- *Administratorem Pani/Pana danych osobowych jest ..... (nazwa firmy) z siedzibą w ..... (dane adresowe),*
- *Dane osobowe zawarte w formularzu kontaktowym będą przetwarzane w celu:*
  a) realizacji zapytania/zgłoszenia na podstawie art. 6 ust. 1 lit. a) RODO,
  b) marketingu własnych produktów lub usług Administratora danych (art. 6 ust. 1 lit. f RODO.)
- *Pani/Pana dane osobowe będą udostępniane tylko podmiotom, którym Administrator ma obowiązek przekazywać dane na gruncie obowiązujących przepisów prawa.*
- *Dane osobowe będą przetwarzane do czasu realizacji celu, dla którego zostały zebrane, a następnie przez okres niezbędny do zabezpieczenia ewentualnych roszczeń związanych z przetwarzaniem danych.*
- *Posiada Pani/Pan prawo dostępu do treści swoich danych, ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.*
- *Posiada Pani/Pan prawo do wniesienia skargi, gdy uzna Pani/Pan, że przetwarzanie danych narusza przepisy RODO Skargę należy wnieść do organu nadzorczego, którym od dnia 25 maja 2018 r. będzie Prezes Urzędu Ochrony Danych Osobowych.*
- *Podanie danych jest dobrowolne, ale niezbędne do realizacji powyższego celu.*

Zgoda

☐ *Wyrażam zgodę na przetwarzanie moich danych osobowych przez ..... w celu realizacji zapytania/zgłoszenia.*

☐ *Wyrażam dobrowolną zgodę na otrzymywanie drogą elektroniczną informacji marketingowych i promocyjnych od ....., na wskazany powyżej numer telefonu i adres poczty elektronicznej.*

11. Powierzenie danych osobowych

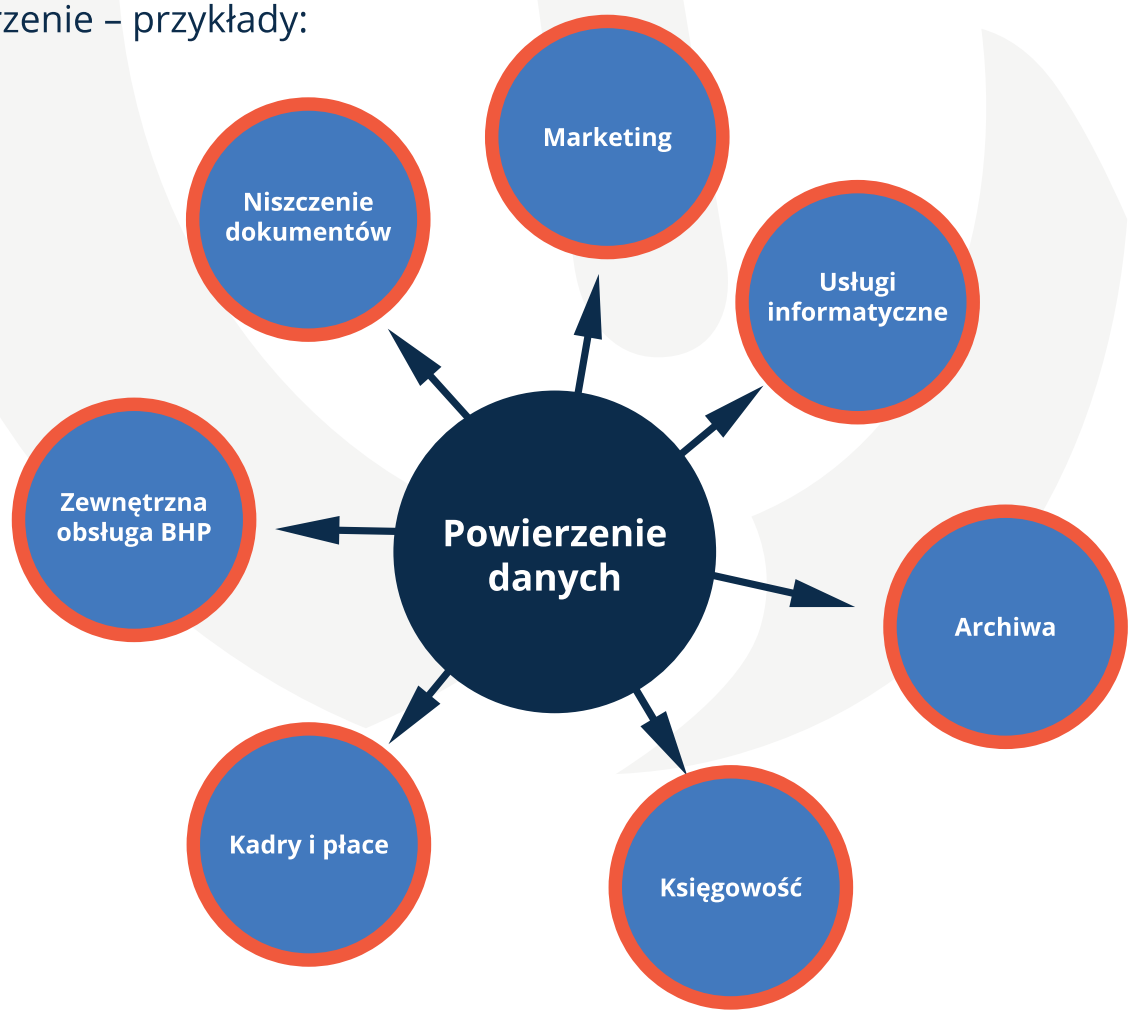
Przetwarzanie danych osobowych można powierzyć również innym podmiotom.
Powierzenie danych to sytuacja, gdy przekazujesz innemu podmiotowi dane osobowe do przetwarzania w sprecyzowanym celu, aby ten podmiot wykonał/ wykonywał określone czynności w imieniu Administratora.
Rosnące znaczenie outsourcingu usług powoduje, że obecnie praktycznie każdy, nawet najmniejszy podmiot korzysta z pomocy zewnętrznych specjalistów (informatyków, prawników, księgowych, etc.).
W takich sytuacjach nierzadko dochodzi do przekazania danych osobowych podmiotom zewnętrznym, np. dokumentacji pracowniczej czy list płac firmie kadrowo-płacowej. Przekazanie to przyjmuje formę powierzenia przetwarzania danych osobowych.

Do powierzenia danych przez ich Administratora nie jest wymagana zgoda osoby, której dane dotyczą, ale jest on zobowiązany zawrzeć w podmiotem przetwarzającym odpowiednią umowę, tzw. umowę powierzenia przetwarzania danych osobowych, w której określone zostaną zasady przetwarzania danych.

Powierzenie przetwarzania danych osobowych powinno odbywać się:

- w oparciu o umowę o powierzeniu przetwarzania danych,
- wyłącznie w zakresie i celu przewidzianym w tej umowie,
- z zapewnieniem, że podmiot, któremu powierzono dane, zabezpiecza je zgodnie z wymaganiami RODO.

Powierzenie – przykłady:

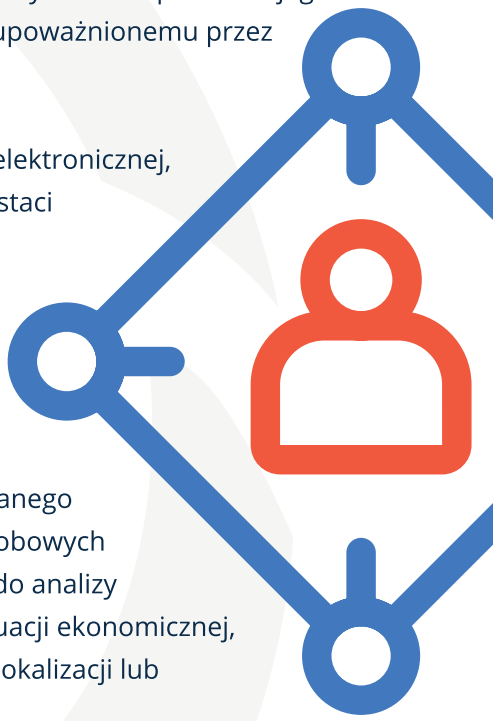


Podmiot przetwarzający dane na zlecenie powinien zawrzeć z Administratorem danych odpowiednią umowę, tzw. umowę powierzenia, w której określone zostaną zasady przetwarzania danych. Każdy podmiot przetwarzający jest zobowiązany do:

a. przetwarzania danych wyłącznie na udokumentowane polecenie Administratora,
b. zapewniania, aby osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,
c. podejmowania środków zabezpieczenia danych wymaganych przez RODO i pomagania Administratorowi wywiązać się z tych obowiązków,
d. przestrzegania warunków korzystania z usług innego podmiotu przetwarzającego – tzw. podpowiedzenie przetwarzania danych jest dopuszczalne wyłącznie za zgodą Administratora danych,
e. pomagania Administratorowi wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w RODO,
f. usunięcia danych lub do zwrotu danych Administratorowi po zakończeniu przetwarzania, zgodnie z jego decyzją,
g. udostępniania Administratorowi wszelkich informacji niezbędnych do wykazania spełnienia jego obowiązków oraz do umożliwiania Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów.

Umowa powierzenia może zostać zawarta w formie pisemnej oraz w formie elektronicznej, pod warunkiem zapewnienia integralności i autentyczności dokumentu w postaci elektronicznej.

12. Co to jest profilowanie danych?



Zgodnie z art. 4 pkt 4 RODO, profilowanie to: “dowolna forma 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”.

RODO wskazuje dwie kategorie profilowania polegające na:

- ocenie prawdziwych informacji pozyskanych na temat danej osoby

albo

- na wytworzeniu nowej informacji o osobie, na podstawie wiedzy pozyskanej na jej temat.

W drugim przypadku nowa informacja będzie jedynie statystycznie prawdziwa, a co za tym idzie pojawia się ryzyko przypisania podmiotowi danych cech, których w istocie on nie posiada, co z kolei doprowadzić może do nieusprawiedliwionej oceny i jej następstw.

RODO przewiduje również dwie formy profilowania:

- profilowanie zwykłe (z udziałem czynnika ludzkiego)
- zautomatyzowane, gdzie cały proces oceny oraz podjęcie decyzji dokonują programy komputerowe (procesy kończące się podjęciem zautomatyzowanej decyzji).

Taki mechanizm stosować wyłącznie wtedy, gdy spełniony jest jeden z następujących warunków:

- osoba profilowana wyrazi na to wyraźną zgodę,
- profilowanie jest niezbędne do zawarcia lub wykonywania umowy z tą osobą,
- profilowanie jest dopuszczalne przez szczególne przepisy prawa.

13. Privacy by design i Privacy by default.

Nowe pojęcia „privacy by design" oraz „privacy by default" wprowadzone przez RODO to inaczej uwzględnienie ochrony danych osobowych w fazie projektowania i uczynienie jej domyślną we wszystkich operacjach związanych z przetwarzaniem. Art. 35 Rozporządzenia nakazuje Administratorowi dokonanie oceny skutków planowanych oraz istniejących operacji przetwarzania dla ochrony danych osobowych w sytuacji, gdy dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Ocena ta powinna zostać dokonana przed rozpoczęciem przetwarzania danych, a zatem jeszcze przed ich otrzymaniem od użytkownika.

14. Zabezpieczanie danych osobowych, analiza ryzyka.

Ocena skutków planowanych operacji przetwarzania dla ochrony danych – ma zastąpić dotychczasowy obowiązek dokonywania zgłoszeń zbiorów danych osobowych do GIODO. Głównym celem DPIA (Data Protection Impact Assessment) jest ustalenie prawdopodobieństwa oraz wagi ryzyka dla praw i wolności osób, które może wiązać się z planowanymi czynnościami przetwarzania, a także wdrożenie środków minimalizujących to ryzyko. Administrator danych samodzielnie ma dokonywać oceny procesów przetwarzania danych osobowych pod kątem ryzyka i oczywiście w pełni odpowiadać za trafność tej oceny oraz podjęcie środków mających na celu minimalizację.

Ryzyko dla ochrony danych osobowych może wynikać z:

- charakteru,
- zakresu,
- kontekstu,
- celów przetwarzania.

Każdy podmiot przetwarzający dane osobowe powinien więc:

a. ustalić, jakie dane osobowe, w jakim charakterze, w jakim celu i w jakim środowisku przetwarza,
b. określić ryzyko naruszenia praw lub wolności osób fizycznych związane z takim przetwarzaniem,
c. dobrać odpowiednie środki zabezpieczenia danych, uwzględniając istniejące możliwości techniczne i własne możliwości finansowe.

RODO wskazuje przykładowe środki techniczne i organizacyjne, które mogą służyć osiągnięciu tego celu, tj. zapewnienia stopnia bezpieczeństwa odpowiadającego ryzyku. Są nimi w szczególności:

- pseudonimizacja i szyfrowanie danych osobowych;
- 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. 35 RODO wskazuje, że DPIA powinno być przeprowadzane, jeżeli dane przetwarzane są w szczególności z użyciem nowych technologii i może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Ocena taka jest wymagana w szczególności w przypadku:

a. systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
b. przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10; lub
c. systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

15. Zasady ochrony danych osobowych

Aby skutecznie chronić dane osobowe należy stosować się do kilku prostych zasad.

Zasada wiedzy koniecznej

Pracujesz na danych, które są niezbędne do wykonywania obowiązków na Twoim stanowisku pracy. Szczegółowy zakres dostępu do danych osobowych reguluje upoważnienie do przetwarzania danych osobowych, które podpisałeś.

Zasada odpowiedzialności za zasoby

Jesteś odpowiedzialny za przetwarzane oraz powierzone Ci informacje oraz zobowiązany do przestrzegania ustanowionych procedur bezpieczeństwa informacji.

Szczegółowy zakres odpowiedzialności zawiera oświadczenie o zachowaniu poufności lub upoważnienie do przetwarzania danych osobowych, które podpisałeś.

Zasada zamkniętego pomieszczenia

Nie zostawiaj osób postronnych samych w pomieszczeniu pod Twoją nieobecność. Koniecznie zamykaj pomieszczenia na klucz przy ich opuszczaniu i nie pozostawiaj kluczy w zamkach.

Zasada czystego biurka

Nie zostawiaj bez nadzoru dokumentów papierowych oraz nośników danych na biurku (płyt CD, DVD, pamięci flash USB itp.).

Zasada czystego kosza

Dokumenty papierowe, z wyjątkiem materiałów promocyjnych, powinny być niszczone w niszczarkach lub za pośrednictwem firmy zewnętrznej.

Zasada czystej tablicy

Po zakończonym spotkaniu w pomieszczeniach ogólnodostępnych (sale konferencyjne itp.) zawsze uprzątnij wszystkie materiały oraz wyczyść tablice (flipchart, itp.).

Zasada czystego ekranu

Blokuj komputer przed każdym opuszczeniem pomieszczenia. W przypadku dłuższej nieobecności w pomieszczeniu, koniecznie wyloguj się z systemu.

Zasada czystego pulpitu

Na pulpicie komputera miej zapisane jedynie ikony standardowego oprogramowania i aplikacji służbowych oraz skróty do folderów pod warunkiem, że w nazwie nie zawierają informacji, które mogą zostać w sposób niekontrolowany ujawnione (np. podczas prezentacji).

Zasada prywatności kont w systemach

Jesteś zobowiązany do pracy w systemach teleinformatycznych na przypisanych Ci kontach. Zabronione jest udostępnianie kont osobom, które nie zostały do nich przypisane.

Zasada poufności haseł i kodów dostępu

Zachowaj poufność i nie przekazuj osobom nieuprawnionym haseł i kodów dostępu. W szczególności zasada ta dotyczy osobistych haseł dostępu do systemów teleinformatycznych i stref chronionych.

Zasada udostępniania danych drogą telefoniczną

Nie udzielaj informacji telefonicznie, jeśli nie jesteś w stanie zidentyfikować osoby, z którą rozmawiasz.

Zasada ograniczonego zaufania

Nie otwieraj wiadomości e-mail, wobec których masz podejrzenia.

Zasady wysyłania danych osobowych mailem

Gdy wysyłasz dane osobowe e-mailem, pamiętaj, aby zabezpieczyć je w należyty sposób. Możesz postąpić według poniższego schematu: zapisać dane w programie archiwizującym, nałożyć na dokument hasło, wysłać e-mail z zabezpieczonym dokumentem, a następnie wysłać SMS-a z hasłem do dokumentu.

Zasada legalności oprogramowania

Zabrania się samodzielnego instalowania oprogramowania, w tym – w szczególności – przechowywania na komputerze treści naruszających prawa autorskie oraz innych nielegalnych danych.

16. Naruszenie bezpieczeństwa danych osobowych

Naruszeniem bezpieczeństwa danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawniania danych osobowych, udostępniania lub umożliwiania dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, również w odniesieniu do systemu informatycznego.

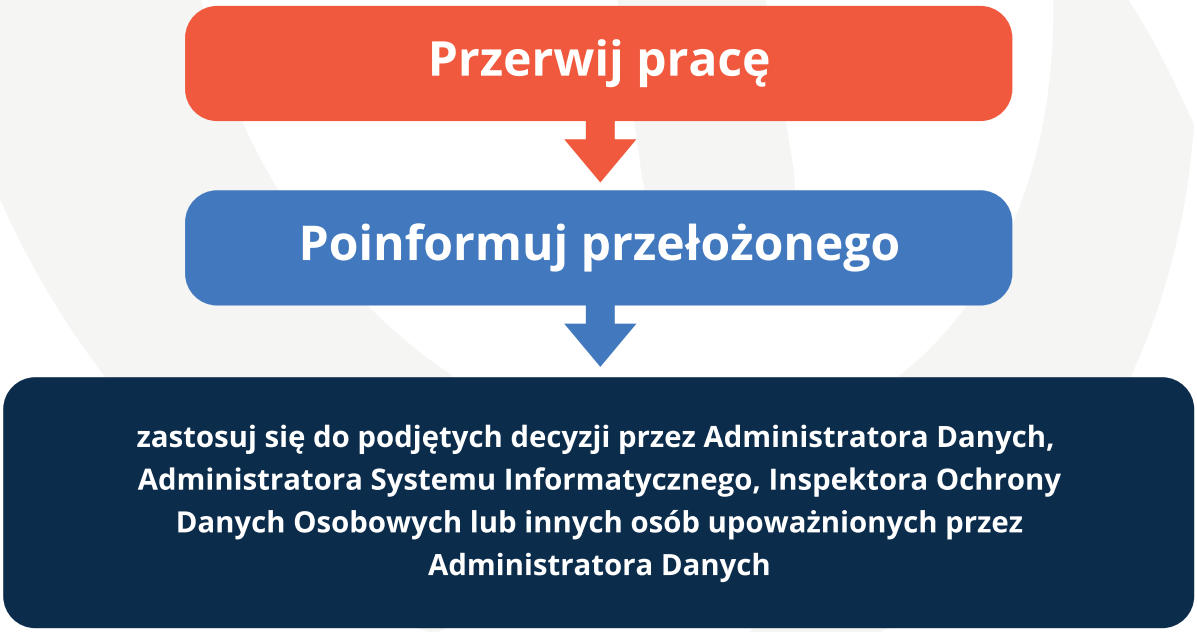
Typowe zagrożenia bezpieczeństwa danych osobowych:

- niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
- niewłaściwe zabezpieczenie sprzętu, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
- nieprzestrzeganie zasad ochrony danych osobowych przez pracowników.

Typowe incydenty bezpieczeństwa danych osobowych:

- zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
- zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych),
- umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

Co zrobić, kiedy dojdzie do naruszenia bezpieczeństwa danych osobowych?



O wystąpieniu incydentu należy poinformować organ nadzorczy (PUODO). Informacja powinna zostać przekazania niezwłocznie, lecz nie później niż w ciągu 72 godzin od stwierdzenia naruszenia.

W pewnych przypadkach należy również informować o incydencie osoby, których dane dotyczą – będzie tak wtedy, gdy naruszenie może powodować wysokie ryzyko naruszenia praw i wolności osoby, której dane dotyczą.

17. Wdrożenie RODO w organizacjach

Skuteczne wdrażanie systemu ochrony danych osobowych zgodnie z wymogami RODO, wymaga zmiana sposobu myślenia o ochronie danych osobowych. Dotychczas wiele podmiotów nie przywiązywało wagi do tych kwestii, ponieważ nie było realnych sankcji. Pozbawione haseł komputery firmowe, przechowywanie w nieskończoność i w sposób niezinwentaryzowany dokumentów zawierających dane osobowe, nieprzekazywanie klientom informacji o ich prawach, pomijanie w umowach klauzul dotyczących przekazywania danych osobowych były codziennymi praktykami.

Aby skutecznie wypełnić nowe obowiązki wynikające z RODO w pierwszej kolejności należy:

1. Zaplanować proces wdrażania systemu ochrony danych osobowych;
2. Wyznaczyć osoby odpowiedzialne za koordynowanie działań oraz nawiązać bliską współpracę z prawnikiem i informatykiem;
9. Przeprowadzić wewnętrzny audyt — każda firma powinna już wiedzieć, jakie dane osobowe posiada w swoich zasobach informatycznych, gdzie i jak są one przechowywane oraz skąd pochodzą;
4. Ocenić ryzyko związane z przetwarzaniem danych osobowych;
5. Przemyśleć rozwiązania organizacyjne i techniczne, które będą wdrażane (np. stworzenie rejestru czynności przetwarzania, nadanie identyfikatorów pracownikom, którzy mają dostęp do danych osobowych, usunięcie danych osobowych przetwarzanych niezgodnie z prawem i wiele innych);
6. Wdrożyć i opisać rozwiązania organizacyjne i techniczne, jak również przygotować założenia potrzebne do stworzenia dokumentacji RODO takiej jak np.: polityka ochrony danych, wzór upoważnienia do przetwarzania danych osobowych, wzór umowy o przetwarzanie danych osobowych i wiele innych;
7. Przygotować dokumentację RODO we współpracy z profesjonalnymi firmami doradczymi świadczącymi wysokiej jakości usługi z zakresu bezpieczeństwa informacji oraz ochrony danych osobowych lub z prawnikami;
8. Wdrożyć proces zapewniający skuteczne monitorowanie i aktualizowanie systemu danych osobowych;
9. Przeszkolić pracowników z zakresu ochrony danych osobowych.

Zobacz jak FORSAFE pomoże Twojej firmie przygotować się do nowych wymogów:

1 Audyt zgodności z RODO

- ustalenie procesów przetwarzania danych osobowych
- określenie ryzyka oraz ocena skutków operacji przetwarzania dla ochrony danych (DPIA)
- weryfikacja i ocena klauzul informacyjnych oraz zgód pod kątem zgodności z RODO
- weryfikacja i ocena stosowanych umów pod kątem powierzenia przetwarzania danych
- ustalenie przekazywania danych osobowych do państw trzecich (poza EOG)
- weryfikacja i ocena systemów informatycznych w których przetwarzane są dane osobowe
- ustalenie i ocena zastosowanych zabezpieczeń fizycznych, informatycznych i organizacyjnych
- opracowanie raportu wraz z rekomendacjami

2 Wdrożenie systemu RODO

- wsparcie we wdrożeniu rekomendacji wynikających z audytu
- opracowanie rejestru kategorii i czynności przetwarzania
- opracowanie klauzul informacyjnych i zgód
- opracowanie wzorcowych umów powierzenia przetwarzania danych
- opracowanie polityki zgłaszania i zarządzania naruszeniami
- opracowanie i wdrożenie dokumentacji przetwarzania danych

3 Nadzór

- weryfikacja procesów i projektów w celu zapewnienia realizacji zasad Privacy by Design i Privacy by Default
- cykliczne sprawdzenia (audyty) procesów przetwarzania danych
- potwierdzenie zgodności

4 Szkolenia

- opracowanie programu szkoleń stacjonarnych i elearningowych
- przeprowadzenie szkoleń dla personelu
- przeprowadzenie testów sprawdzających
- wydanie zaświadczeń

18. Szkolenia e-learningowe

Rewolucja w Ochronie Danych Osobowych staje się faktem.

Wdrożenie RODO w Organizacjach – e-szkolenie dla Przedsiębiorców i Pracowników.

Cel szkolenia

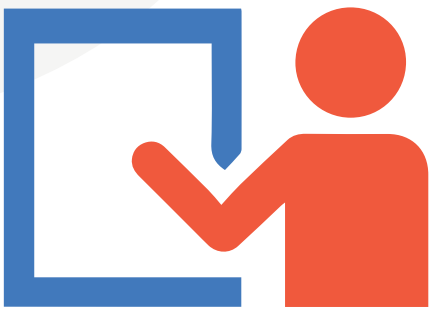
Zaznajomienie uczestników z przepisami nowego Europejskiego Prawa Ochrony Danych Osobowych („RODO" lub „GDPR"), ważnymi od 25 maja 2018 r. pod kątem prawnym i organizacyjno-technicznym.

Dlaczego to jest ważne?

Zgodnie z RODO Administratorzy Danych stają przed wyzwaniem wdrożenia odpowiednich środków technicznych i organizacyjnych, które w najlepszy sposób ochronią dane osobowe przed incydentami związanymi z ich bezpieczeństwem. **Jednym z możliwych do zastosowania środków organizacyjnych jest obowiązkowe e-szkolenie dla pracowników.**

Zagadnienia poruszane na szkoleniu:

- Podstawa prawna ochrony danych osobowych.
- Podstawowe pojęcia z zakresu ochrony danych osobowych.
- Zasady dotyczące przetwarzania danych osobowych.
- Prawa osób, których dane dotyczą.
- Obowiązki Administratora Danych.
- Status i zadania Inspektora Ochrony Danych.
- Zasady przetwarzania danych w imieniu Administratora Danych.
- Przekazywanie danych osobowych.
- Środki ochrony prawnej.



E-szkolenia od Forsafe

E-lastyczność

pracownik szkoli się wtedy, kiedy ma na to czas
- dostęp do szkolenia 24/7.

E-fektywność

wiedza jest przyswajana samodzielne i w dogodnym tempie.

E-konomia

niski koszt dla Pracodawców, możliwość przeszkolenia wielu pracowników w krótkim czasie.

E-dukacja

szkolenie zawiera ciekawe ćwiczenia pozwalające utrwalić wiedzę

E-waluacja

każdy uczestnik otrzymuje imienny certyfikat po zakończeniu szkolenia potwierdzający zdobytą wiedzę.

Aby uzyskać dostęp do naszych e-szkoleń wejdź na stronę

www.forsafe.pl/e-szkolenia

FORSAFE

BEZPIECZEŃSTWO PONAD WSZYSTKO

FORSAFE Sp. z o.o.

ul. 1 Maja 31/33,
90-739 Łódź

tel. +48 42 631-95-62
kom. 600-005-880

e-mail: biuro@forsafe.pl