Szkolenie dotyczące przestrzegania przepisów o ochronie danych osobowych w Nexpertis

CZYM JEST RODO

RODO (ang. GDPR) - Ogólne Rozporządzenie o Ochronie Danych Osobowych (Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r.) jest nowym aktem prawnym regulującym ochronę prywatności na terytorium UE. Celem RODO jest zapewnienie i zwiększenie kontroli osób fizycznych nad swoimi własnymi danymi osobowymi. W tym celu RODO nakłada nowe obowiązki na podmioty zbierające (gromadzące), przechowujące i przetwarzające dane osobowe.

RODO weszło w życie w dniu 24 maja 2016 r., jednakże państwa członkowskie UE do dnia 24 maja 2018 r. mają czas na wprowadzenie regulacji ustawowych realizujących postanowienia RODO. Po dniu 25 maja 2018 r. RODO będzie stosowana bezpośrednio w tych krajach członkowskich, które nie wprowadziły regulacji ustawowych w tym zakresie. **Tym samych w zakresie regulowanym RODO nie będzie stosowana UODO - ustawa z dnia 29 sierpnia 1997 r. o ochronie osobowych (Dz.U. z 2016 r., poz. 922 – t.j.)**

CO JEST CELEM RODO

Celem RODO jest zwiększenie ochrony osób fizycznych w zakresie zbierania, przechowania i przetwarzania ich danych osobowych, w szczególności poprzez:

- ✓ zapewnienie dostępu do własnych danych osobowych,
- ✓ umożliwienie usunięcia własnych danych osobowych,
- ✓ udostępnienie własnych danych osobowych w celu ich edycji (poprawa błędów, wprowadzenie zmian), zapewnienie prawa do odmowy przetwarzania własnych danych osobowych.

CO WPROWADZA RODO W STOSUNKU DO REGULACJI KRAJOWYCH CZYLI USTAWY O OCHRONIE DANYCH OSOBOWYCH

- ✓ RODO jest regulacją UE – ujednolica więc zasad przetwarzania danych w całej UE,
- ✓ Wprowadza wymóg prowadzenia rejestru
- ✓ Wprowadza czynności przetwarzania danych,
- ✓ Wprowadza obowiązek zgłoszenia naruszenia ochrony danych w terminie nie dłuższym niż 72h od naruszenia,
- ✓ rozszerza katalog danych o dane genetyczne i biometryczne,
- ✓ wprowadza privacy by design,
- ✓ wprowadza prawo do: przenoszenia i edycji danych , sprzeciwu i roszczenia odszkodowawcze.

JAKIE NOWE POJECIA WPROWADZA RODO:

- ✓ Przejrzystość i Zgoda - tj. informacje, które należy przekazać i zgody, które należy uzyskać od osób, których dane dotyczą, w celu uzasadnienia wykorzystywania tych danych. Wymogi RODO, w tym w zakresie zgody, która musi być jednoznaczna i nie może być domniemana na podstawie braku działania, oznaczają, że wiele informacji przekazanych osobom fizycznym dotyczących ochrony danych będzie wymagało poprawek.
- ✓ Dzieci i zgoda - wyrażona cyfrowo zgoda rodziców wymagana jest w przypadku wykorzystywania danych osoby poniżej 13 roku życia. Państwa członkowskie mają swobodę ustanawiania własnych zasad w odniesieniu do osób w wieku od 13 do 15 lat (włącznie). Jeśli jednak nie skorzystają z tego prawa, zgoda rodziców będzie wymagana dla wszystkich dzieci poniżej 16 roku życia.
- ✓ Dane regulowane - definicje „danych osobowych" i „danych wrażliwych" zostały rozszerzone, dla przykładu ta ostatnia obejmuje teraz dane genetyczne i biometryczne.
- ✓ Pseudonimizacja - technika zwiększająca ochronę prywatności polegająca na tym, że informacje pozwalające na przypisanie danych do określonych osób są przechowywane oddzielnie i z zastosowaniem technicznych i organizacyjnych środków zapewniających, że dane nie zostaną ze sobą skojarzone.
- ✓ Naruszenie ochrony danych osobowych - nowe obowiązki w zakresie powiadamiania o naruszeniu bezpieczeństwa danych zostaną wprowadzone w odniesieniu do wszystkich administratorów danych, bez względu na sektor.
- ✓ Uwzględnianie ochrony danych w fazie projektowania i rozliczalność - organizacje mają obowiązek wdrożenia znacznej liczby nowych środków technicznych i organizacyjnych w celu wykazania zgodności z RODO.
- ✓ Zwiększone prawa – osoby, których dane dotyczą, otrzymują nowe, szersze uprawnienia, w tym prawo do bycia zapomnianym, prawo do przenoszenia danych i prawo do sprzeciwu wobec zautomatyzowanego podejmowania decyzji.
- ✓ Współpraca miedzy organem nadzorczym a Europejską Radą Ochrony Danych - nadzór regulacyjny nad ochroną danych ulegnie zmianie w znacznym stopniu, w tym na skutek m.in. wprowadzenia organów wiodących dla niektórych jednostek organizacyjnych

CO TO SĄ DANE OSOBOWE WEDŁUG RODO i UODO

RODO	UODO
Zgodnie z art. 4 ust. 1 RODO – Dane osobowe, to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej	Zgodnie z art. 6 ust. 1 UODO – Dane osobowe, to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej

RODO i UODO nie definiują pojęcia osoby zidentyfikowanej (brak definicji legalnej). Zgodnie z przyjętą praktyką osobą zidentyfikowaną jest osoba, co do której nie trzeba przeprowadzać identyfikacji, ponieważ jej tożsamość jest już znana - administrator danych osobowych ma możliwość powiązania posiadanej informacji z konkretną osobą, bez konieczności podejmowania dalszych działań.

CO TO JEST OSOBA MOŻLIWA DO ZIDENTYFIKOWANIA WEDŁUGO PRAWA

art. 6 ust. 2 UODO – osobą możliwą do zidentyfikowania jest osoba, której tożsamości można określić bezpośrednio lub pośrednio, w szczególności poprzez powołanie się na: numer identyfikacyjny, kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, kulturowe lub społeczne	art. 4 ust. 1 RODO – możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak: – imię i nazwisko, – numer identyfikacyjny, – dane o lokalizacji, – identyfikator internetowy – jeden lub kilka szczególnych czynników określających: • fizyczną, fizjologiczną, genetyczną, psychiczną, • ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej; motyw 30 preambuły (RODO) – osobom fizycznym mogą zostać przypisane identyfikatory internetowe – takie jak adresy IP, identyfikatory plików cookie generowane przez ich urządzenia, aplikacje, narzędzia i protokoły, czy też inne identyfikatory, generowane na przykład przez etykiety RFID. Może to skutkować zostawieniem śladów, które w szczególności w połączeniu z unikatowymi identyfikatorami i innymi informacjami uzyskiwanymi przez serwery mogą być wykorzystywane do tworzenia profili i identyfikowania tych osób

CO TO JEST PSEUDOANIMIZACJA

Jest to nowa definicja, która odwołuje się do techniki przetwarzania danych osobowych w taki sposób aby nie można ich było przypisać do określonej „osoby której dane dotyczą" bez dodatkowych informacji, które muszą być przechowywane oddzielnie i z zastosowaniem technicznych i organizacyjnych środków zapewniających, że dane nie zostaną ze sobą skojarzone.

WAŻNE: Informacje spseudonimizowane nadal stanowią dane osobowe, jednak zaleca się stosowanie tej techniki, w szczególności w przypadku:

- ✓ gdy jest to czynnik do rozważenia przy określaniu, czy przetwarzanie jest „niezgodne" z celem, dla którego dane osobowe były pierwotnie zbierane i przetwarzane;
- ✓ gdy może ona przyczynić się do spełnienia wymogu „uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych"
- ✓ gdy może ona przyczynić się do wypełnienia przewidzianych w RODO obowiązków w zakresie bezpieczeństwa danych (więcej informacji w części poświęconej naruszeniom ochrony danych osobowych i ich zgłaszaniu); oraz

- ✓ w przypadku organizacji zamierzających wykorzystywać dane osobowe dla potrzeb badań historycznych lub naukowych, lub też dla celów statystycznych, podkreśla się przydatność techniki pseudonimizacji.

NA CZYM POLEGA UWZGLEDNIENIE OCHRONY DANYCH W FAZIE PROJEKTOWANIA

- ✓ Organizacje muszą być w stanie wykazać zgodność z przepisami RODO, w tym poprzez przyjęcie pewnych środków w zakresie „uwzględniania ochrony danych w fazie projektowania" (np. zastosowanie techniki pseudonimizacji), przeprowadzenie szkolenia pracowników i przeprowadzenie audytów.
- ✓ W przypadku przetwarzania o „wysokim stopniu ryzyka" (np. monitorowanie, regularne oceny lub przetwarzanie szczególnych kategorii danych osobowych), należy przeprowadzić i udokumentować szczegółową ocenę skutków dla ochrony danych. W przypadku, gdy wynik wyżej wspomnianej oceny wskazuje, że istnieje wysokie i niczym niezminimalizowane ryzyko dla osób, których dane dotyczą, administratorzy danych muszą powiadomić organ nadzorczy i uzyskać jego opinię na temat adekwatności środków zaproponowanych w ocenie skutków dla ochrony danych w celu zmniejszenia ryzyka związanego z przetwarzaniem danych.
- ✓ Administratorzy i podmioty przetwarzające dane mogą powołać inspektora ochrony danych. Jest to obowiązkowe w przypadku jednostek sektora publicznego oraz podmiotów wykonujących pewne działania o charakterze wrażliwym lub monitorowania oraz gdy prawo krajowe tego wymaga Spółki powiązane mogą wspólnie powoływać inspektora ochrony danych.

CO TO SA ZWIĘKSZONE PRAWA DLA OSÓB FIZYCZNYCH

RODO kładzie szczególny nacisk na zakres istniejących i nowych praw przysługujących osobom fizycznym w odniesieniu do ich danych osobowych.
Prawa te obejmują prawo do bycia zapomnianym, prawo do żądania przeniesienia danych osobowych do nowego usługodawcy, prawo do sprzeciwu wobec niektórych czynności w zakresie przetwarzania danych, oraz prawo do sprzeciwu wobec zautomatyzowanego podejmowania decyzji

JAK DŁUGO MOŻNA PRZECHOWYWAC DANE OSOBOWE WEDŁUG RODO

- ✓ w przypadku, gdy przetwarzanie danych odbywa się na podstawie udzielonej zgody – może trwać tak długo, aż zgoda zostanie odwołana.
- ✓ w przypadku, gdy przetwarzanie odbywa się na podstawie umowy – może trwać to tak długo jak jest to niezbędne do wykonania wspomnianej umowy.

Oznacza to, że : przetwarzać dane możemy tak długo, jak długo istnieje cel przetwarzania tych danych lub do momentu, kiedy osoba nie zażąda zaprzestania ich przetwarzania. Przykładowo jeśli przy rekrutacji zbierane są CV kandydatów, to dane należy usunąć zaraz po zakończeniu rekrutacji, chyba, że ktoś wyraził zgodę na przetwarzanie swoich danych w celach przyszłej rekrutacji

ILE DANYCH OSOBOWYCH MOŻNA ZBIERAĆ

- ✓ RODO wprowadza zasadę minimalizacji danych osobowych. Można przetwarzać dane tylko te, które są niezbędne do osiągnięcia celu ich przetwarzania.

Innymi słowy: przetwarzanie danych osobowych powinno być ograniczone tylko do tych danych, bez których realizacja celu jest niemożliwa.

Przykład: jeśli Nexpertis proponuje przeprowadzenie dla swoich klientów szkolenia ich kluczowego personelu które to szkolenie dotyczy wdrożonego systemu ,to Nexpertis jako procesor nie może przetwarzać danych dotyczących uczestników szkolenia które zawierają np. wiek takich kursantów ich narodowość, płeć lub pochodzenie etniczne a jedynie może przetwarzać dane niezbędne do wykonania usługi szkolenia. Chyba, że Nexpertis uzyska stosowne i odrębne uprawnienia od tej

PODSTAWOWE OBOWIĄZKI CIĄŻĄCE NA ADMINISTRATORZE

RODO nakłada na administratorów obowiązek przyjęcia środków technicznych i organizacyjnych w celu sprostania obowiązków wynikających z RODO (a także w celu wykazania, że zostało to zrobione). Prowadzenie programu regularnych audytów w połączeniu z innymi środkami, o których mowa poniżej (w szczególności oceną skutków dla ochrony danych), wydaje się być dobrze widziane przez organy nadzorcze odpowiedzialne za egzekwowanie zobowiązań przewidzianych przez RODO.

LISTA OBOWIĄZKÓW ADMINISTRATORA

1. Uwzględnienie ochrony danych w fazie projektowania
   Administrator musi wdrożyć techniczne i organizacyjne środki aby wykazać, że dokonały oceny i wdrożyły środki ochrony w obrębie swoich działań przetwarzania danych.
2. Dokonanie oceny skutków dla ochrony (co oznacza ocena mająca za zadanie identyfikację i minimalizację ryzyka niezgodności. W szczególności, administratorzy muszą zapewnić, że ocena skutków dla ochrony danych została przeprowadzona dla każdej czynności przetwarzania „o wysokim ryzyku", zanim czynność ta została podjęta -mierzonej w odniesieniu do ryzyka naruszenia praw i wolności osoby fizycznej.
   a) Przetwarzanie o wysokim ryzyku obejmuje:
      (i) systematyczne i kompleksowe czynności przetwarzania, w tym profilowanie, które są podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób istotnie wpływających na osobę fizyczną,
      (ii) (przetwarzanie na dużą skalę szczególnych kategorii danych osobowych lub danych dotyczących wyroków skazujących i naruszeń prawa lub
      (iii) Systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie (monitoring wizyjny).

KTO TO JEST PROCESOR:

Procesor to podmiot (osoba fizyczna lub prawną, organ publiczny, jednostka) lub inny podmiot, który przetwarza powierzone dane osobowe w imieniu administratora.

Procesor nie przetwarza danych dla swoich celów, wykonuje on jedynie zadanie zlecone mu przez administratora danych.

W JAKI SPOSÓB MOŻE DOJŚĆ DO PRZETWARZANIA DANYCH OSOBOWYCH PRZEZ PROCESORA

Aby doszło do przetwarzania danych osobowych przez podmiot przetwarzający, musi zostać zawarta umowa powierzenia przetwarzania danych. Niezbędne jej elementy to: określenie przedmiotu, czas trwania umowy, charakter i cel przetwarzania, oznaczenie obowiązków i praw administratora, a także

rodzajów danych osobowych oraz kategorii osób, których dane te dotyczą. RODO wprowadza możliwość zawierania takich umów także w formie elektronicznej .

Rozporządzenie wymaga, aby administrator powierzał przetwarzanie danych osobowych wyłącznie takim podmiotom, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, dzięki którym przetwarzanie będzie zgodne z przepisami rozporządzenia i będzie chroniło prawa osób, których

ZAKRES ZMIAN W RELACJI PROCESOR DANYCH OSOBOWYCH I ADMINISTRATOR DANYCH

RODO nakłada ograniczenia na procesorów danych poprzez .

- ✓ zakaz podpowierzania przetwarzania danych osobowych innym podmiotom bez pisemnej zgody administratora tych danych.
- ✓ możliwość przetwarzania powierzonych danych wyłącznie na udokumentowane polecenie administratora tych danych. Innymi słowy procesor musi gromadzić i przechowywać polecenia administratora danych tak by mógł udowodnić, że sam nie podjął decyzji o zmianie sposobu czy też celu przetwarzania danych osobowych lub choćby przesłania danych osobowych do Państwa trzeciego. Jeżeli jednak okaże się, że procesor danych zmieni np. cel przetwarzania danych to automatycznie staje się administratorem tych danych i ponosi pełną odpowiedzialność niejako w zastępstwie pierwotnego administratora danych.
- ✓ konieczność zapewnienia by osoby które zostały upoważnione do przetwarzania powierzonych danych osobowych zachowały je w tajemnicy.
- ✓ nałożenie odpowiedzialności za odpowiedni poziom bezpieczeństwa wdrożony po stronie podmiotu, któremu procesor podpowierzył przetwarzanie danych osobowych. Innymi słowy jeżeli podprocesor nie zapewni odpowiednich zabezpieczeń zgodnie z treścią Rozporządzenia UE, odpowiedzialność za jego braki poniesie ten podmiot, który mu podpowierzył dane, a nie sam administrator danych
- ✓ współpraca z administratorem danych w wywiązywaniu się z obowiązku odpowiadania na żądania osób, których dane dotyczą. W praktyce będzie musiał współdziałać z administratorem danych w zakresie realizacji uprawnień osób, których dane dotyczą.
- ✓ obowiązek usunięcia danych lub zwrotu ich administratorowi danych, po zakończeniu przetwarzania powierzonych danych. Procesor będzie miał w zależności od jego woli. Obowiązek ten dotyczy również wszelkich kopii danych, które zostały wykonane.

Ostatecznie procesor danych udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w przepisach Rozporządzenia ogólnego UE oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich. Przepis ten domyślnie zakłada możliwość przeprowadzenia kontroli po stronie procesora danych z inicjatywy administratora danych.

Procesor będzie musiał wyznaczać Inspektora ochrony danych (IOD) w sytuacji, gdy współpracuje z administratorami, którzy muszą wyznaczyć IOD.

CZY OSOBY KTÓRE PROWADZĄ WŁASNĄ DZIAŁALNOŚC GOSPODARCZĄ DZIAŁAJĄ W STRUKTURZE ORGANIZATORA CZY SĄ PROCESORAMI

- ✓ Przy przekazywaniu danych osobowych poza strukturę organizacyjną jednego podmiotu – w tym przypadku administratora - wymagane jest zawieranie umów powierzenia danych osobowych, które legalizują taki transfer danych. W związku z tym ze współpracownikami powinno zawierać się umowy powierzenia przetwarzania danych osobowych i traktować ich jako procesorów. Jako przedsiębiorcy - podmioty profesjonalne - współpracownicy będą odpowiedzialni za naruszenia ochrony danych osobowych bądź na zasadach przewidzianych w przepisach prawa cywilnego, bądź na zasadach przewidzianych w umowie regulującej współpracę.
- ✓ Osoby zatrudnione na umowę-zlecenie lub umowę o dzieło powinny być traktowane jak osoby włączone do struktur organizacyjnych administratora. Można więc takie osoby upoważnić do przetwarzania danych osobowych na zasadach analogicznych jak obowiązujące etatowych pracowników. Wówczas przetwarzają oni dane osobowe z polecenia administratora. A ten odpowiada bezpośrednio za ich ewentualne błędy. Przy czym może jednak żądać od takich osób pokrycia wynikłej z błędu szkody bądź na zasadach przewidzianych w przepisach prawa cywilnego, bądź na zasadach określonych w umowie.

KTO TO JEST IOD I KIEDY ISTNIEJE OBOWIAZEK POWOŁANIA GO W FIRMIE:

IOD to Inspektor Ochrony Danych

Zgodnie z art. 37 RODO, w niektórych przypadkach wyznaczenie takiego IOD jest obligatoryjne, zarówno dla administratora jak i procesora. Mogą jednak wystąpić sytuacje, kiedy administrator nie będzie zobowiązany do wyznaczenia DPO, natomiast obowiązek taki będzie ciążył na podmiocie przetwarzającym. Unijna Grupa Robocza art. 29 udzielająca opinii w ważnych sprawach dotyczących ochrony danych osobowych, opisuje sytuację, w której mała, rodzinna firma dystrybuuje artykuły gospodarstwa domowego na terenie jednego miasta. Rodzina korzysta z usług Procesora, którego podstawowa działalność polega na świadczeniu usług analityki internetowej i pomocy w ukierunkowanej reklamie i marketingu. Działalność firmy rodzinnej, biorąc pod uwagę niewielką liczbę klientów i stosunkowo ograniczone działania, nie spowoduje obowiązku wyznaczania IDO. Jednakże działania podmiotu przetwarzającego, posiadającego wielu klientów takich jak to małe przedsiębiorstwo, kwalifikuje się jako przetwarzanie „na dużą skalę". W związku z tym podmiot przetwarzający, w przeciwieństwie do lokalnego przedsiębiorstwa, zobowiązany będzie do wyznaczenia inspektora ochrony danych.

NARUSZENIE DANYCH, ICH ZGŁASZANIE i SPOSOBY POSTĘPOWANIA

1. Podmioty przetwarzające dane są zobowiązane zgłaszać naruszenia ochrony danych do administratorów danych.
2. Administratorzy danych z kolei są zobowiązani zgłaszać naruszenia ochrony danych do organów nadzorczych, którym podlegają, a w pewnych przypadkach zawiadamiać także do osoby, których dane dotyczą, w każdym przypadku postępując zgodnie z przepisami RODO.
3. Administratorzy danych osobowych są zobowiązani prowadzić wewnętrzny rejestr naruszeń ochrony danych.

CO TO SA INCYDENTY I KIEDY POWODUJĄ OBOWIĄZEK ZGŁOSZENIA NARUSZENIA

W przypadku zajścia incydentu określanego, jako „naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych,

przechowywanych lub w inny sposób przetwarzanych", nowe przepisy ogólne w sprawie zgłaszania naruszenia ochrony danych, wprowadzone na mocy RODO, będą obowiązywać w następujący sposób:

1. Obowiązek podmiotów przetwarzających dane do powiadomienia administratora danych

Termin:

Bez zbędnej zwłoki po powzięciu wiedzy o zdarzeniu.

Odstępstwo:

Brak na gruncie RODO

Wnioski:

Wszystkie naruszenia będzie trzeba zgłaszać.

2. Obowiązek administratorów danych osobowych do powiadomienia organów nadzorczych

Termin:

Bez zbędnej zwłoki oraz, w miarę możliwości, nie później, niż 72 godziny po zasięgnięciu wiedzy o zdarzeniu.

Odstępstwo:

Brak obowiązku zgłaszania w przypadku, gdy naruszenie nie jest związane z ryzykiem naruszenia praw i wolności osób fizycznych.

Wnioski:

W przypadku uchybienia terminom zgłoszenia, będzie konieczne wyjaśnienie sytuacji organom nadzorczym

(np. żądanie ze strony organu wymiaru sprawiedliwości)

3. Obowiązek administratorów danych osobowych powiadomienia osób, których dane dotyczą, o naruszeniu ochrony danych osobowych

W przypadku, gdy działanie takie nie zostało podjęte, organ nadzorczy może zobowiązać administratora danych osobowych do powiadomienia o naruszeniu ochrony danych osobowych osób, których dane dotyczą, chyba że zastosowanie ma jedno z trzech odstępstw.

Termin:

Bez zbędnej zwłoki: konieczność zminimalizowania natychmiastowego ryzyka szkód wymaga szybkiego kontaktu z osobami, których dane dotyczą, natomiast konieczność wdrożenia odpowiednich środków przeciwko trwającym lub podobnym naruszeniom ochrony danych może uzasadniać dłuższy okres na zgłoszenie.

Odstępstwo:

Brak konieczności zgłaszania w przypadku:

- ✓ gdy naruszenie nie jest związane z ryzykiem naruszenia praw i wolności osób, których dane dotyczą, albo takie ryzyko jest niższe niż wysokie;

- ✓ gdy odpowiednie techniczne i organizacyjne zabezpieczenia były wdrożone w chwili zajścia incydentu (np. szyfrowanie danych); lub
- ✓ gdyby spowodowało to konieczność podjęcia nieproporcjonalnie dużych starań (zamiast tego powinno się organizować publiczne kampanie informacyjne w celu skutecznego informowania dotkniętych problemem osób)

NARUSZENIE DANYCH I ICH ZGŁASZANIE i SPOSOBY POSTĘPOWANIA

- ✓ Podmioty przetwarzające dane są zobowiązane zgłaszać naruszenia ochrony danych do administratorów danych.
- ✓ Administratorzy danych z kolei są zobowiązani zgłaszać naruszenia ochrony danych do organów nadzorczych, którym podlegają, a w pewnych przypadkach zawiadamiać także do osoby, których dane dotyczą, w każdym przypadku postępując zgodnie z przepisami RODO.
- ✓ Administratorzy danych osobowych są zobowiązani prowadzić wewnętrzny rejestr naruszeń ochrony danych.

CO ADMINISTRATOR POWINIEN ZROBIĆ ABY ZARADZIĆ NARUSZENIOM:

- ✓ Zapewnić, że wdrożone zostaną odpowiednie techniczne i organizacyjne zabezpieczenia, które spowodują, że w przypadku dostępu osób nieupoważnionych dane staną się niemożliwe do odczytania.
- ✓ Dokonać przeglądu polis ubezpieczeniowych aby ocenić zakres ochrony, jaką zapewniają w przypadku naruszenia ochrony danych.
- ✓ Uaktualnić wzory umów ramowych / klauzul ochrony danych oraz dokumentacji przetargowej powinny zostać uaktualnione, w szczególności w zakresie w tym:
    - w celu zobowiązania dostawców do aktywnego zgłaszania naruszeń ochrony danych
    - położenia większego nacisku na obowiązek współpracy pomiędzy stronami

JAK USTALIĆ KTÓRE NARUSZENIA OCHRONY DANYCH NALEŻY ZGŁOSIĆ?

Artykuł 4 pkt 12 RODO stanowi, że naruszenie ochrony danych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych. Pomocne w ocenie naruszeń mogą być także wyjaśnienia zawarte w Wytycznych Grupy Roboczej art. 29 w sprawie powiadomień o naruszeniu ochrony danych osobowych na mocy rozporządzenia 2016/670 przyjętych 3 października 2017 r. Zatem administrator, dokonując oceny danego zdarzenia, będzie mógł się nimi posiłkować. UODO nie jest zaś uprawniony, by konsultować zaistniałe incydenty z administratorem. RODO określa, że zgłoszenie naruszenia ma nastąpić niezwłocznie, jednak nie później niż w ciągu 72 godzin od wykrycia. Ten termin jest wystarczająco długi, by w większości przypadków przeanalizować, czy faktycznie doszło do naruszenia, a jeśli tak, to jakie są lub mogą być jego skutki i jakie należy podjąć działania zaradcze.

Wyjątkowo administrator może zgłosić naruszenie po upływie 72 godzin. Jednak wówczas musi przesłać również wyjaśnienie przyczyn opóźnienia. Należy pamiętać, że działania związane z naruszeniem ochrony danych powinny być podejmowane szybko. Chodzi o to, by w jak najkrótszym czasie wdrożyć rozwiązania zabezpieczające, by możliwie szybko ograniczyć skutki np. wycieku danych, zabezpieczyć inne dane oraz podjąć odpowiednie działania naprawcze, a także wówczas, gdy to konieczne, poinformować o zaistniałej sytuacji osoby, których dane dotyczą.

JAK ODPOWIEDNIO ZABEZPIECZYĆ DANE?

RODO odchodzi od praktyki wskazywania konkretnych środków zabezpieczenia danych osobowych. Jakie zatem zabezpieczenia zastosować? Jak prezes UODO będzie oceniał, czy przedsiębiorca zastosował właściwe środki?

W RODO nie znajdziemy podpowiedzi, jakie działania należy podjąć, aby takie ryzyko ocenić, ani żadnej metodyki w tym zakresie. RODO stanowi jednak, że przy ocenie ryzyka i ustanawianiu zabezpieczeń minimalizujących to ryzyko należy uwzględnić stan wiedzy technicznej, koszt wdrażania, a także skutki, jak zidentyfikowane zagrożenia mogą wpływać na naruszenie praw i wolność osób, których dane są przetwarzane.

Uwzględnienie kontekstu przetwarzania danych to niezbędny element podejścia opartego na ryzyku. Tylko pełne informacje o kontekście użycia danej informacji pozwolą na rzetelną ocenę skutków związanych z ich brakiem, przekłamaniem lub nieuprawnionym ujawnieniem. Kontekst to również czynniki, które mogą spowodować utratę, nieuprawnione wykorzystanie lub brak dostępu do przetwarzanych danych.

JAKIE KARY GROŻĄ ZA NIEPRZESTRZEGANIE RODO?

- ✓ Postanowienia RODO przewidują dwa zestawy maksymalnych progów dla administracyjnych kar pieniężnych, które mogą być nakładane za określone naruszenia.
- ✓ W każdym przypadku, maksymalna wysokość kary jest wyrażona w euro lub, w przypadku przedsiębiorstw, jako procent całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, w zależności od tego, która kwota jest wyższa. Motyw 150 RODO potwierdza, że w powyższym kontekście „przedsiębiorstwo" należy rozumieć według definicji zawartej w art. 101 i 102 Traktatu o funkcjonowaniu Unii Europejskiej („TFUE"), tj. ogólnie rzecz ujmując, jako podmioty prowadzące działalność gospodarczą

Sankcja I :

Kara do 10 milionów euro lub do 2% wartości rocznego światowego obrotu przedsiębiorstwa za naruszenie następujących obowiązków:

- ✓ obowiązku uzyskania zgody na przetwarzanie danych dotyczących dzieci (art. 8);
- ✓ obowiązków w zakresie wdrażania nowych środków technicznych i organizacyjnych w celu uwzględnienia ochrony danych w fazie projektowania i domyślnej ochrony danych (art. 25)
- ✓ obowiązków ustalenia zakresu swoich obowiązków dotyczących ochrony danych osobowych przez współadministratorów danych (art. 26);
- ✓ obowiązków nałożonych na administratorów danych i podmioty przetwarzające dane nieposiadających jednostki organizacyjnej na terytorium UE w zakresie wyznaczania przedstawicieli (art. 27);
- ✓ obowiązków nałożonych na administratorów danych w zakresie angażowania podmiotów przetwarzających dane (Art. 28);

- ✓ obowiązków nałożonych na podmioty przetwarzające dane w zakresie angażowania podwykonawców wyłącznie za uprzednią zgodą administratora danych oraz zgodnie z jego instrukcjami (art. 28-29);
- ✓ obowiązków w zakresie prowadzenia pisemnych rejestrów czynności przetwarzania (art. 30);
- ✓ obowiązków nałożonych na podmioty przetwarzające dane w zakresie współpracy z organami nadzorczymi (art 31);
- ✓ obowiązków w zakresie wdrażania środków technicznych i organizacyjnych (art. 32);
- ✓ obowiązków w zakresie zgłaszania naruszeń zgodnie z wymogami RODO (Art. 33-34);
- ✓ obowiązków w zakresie prowadzenia ocen skutków dla ochrony danych (Art. 35-36)
- ✓ obowiązków w zakresie powoływania inspektorów ochrony danych (Art. 37-39)
- ✓ obowiązków nakładanych na podmioty certyfikujące (art. 42-43); oraz
- ✓ obowiązków nakładanych na organy monitorujące w zakresie podejmowania działań w odpowiedzi na naruszenie kodeksów postępowania (art. 41).

Sankcja II:

Kara do 20 milionów euro lub do 4% wartości rocznego światowego obrotu przedsiębiorstwa za naruszenie:

- ✓ zasad dotyczących przetwarzania danych osobowych (art. 5 RODO),
- ✓ warunków wyrażenia zgody na przetwarzanie danych (art. 7 RODO)
- ✓ naruszenie wykonania prawa dostępu przysługującego osobie, której dane dotyczą (art. 15 RODO),
- ✓ naruszenie wykonania prawa do sprostowania i usuwania danych (art. 16 RODO)
- ✓ transgranicznego przekazywania danych (art. 44-49);
- ✓ obowiązków wynikających z prawa państwa członkowskiego przyjętych na podstawie Rozdziału IX; oraz
  nieprzestrzegania poleceń wydanych przez organy nadzorcze (określonych w art. 58(2)) niezastosowanie się do postępowania prowadzonego przez organ nadzorczy na podstawie art. 58(1)

W przypadkach, gdy te same lub powiązane ze sobą operacje przetwarzania danych są związane z naruszeniem więcej, niż jednego przepisu RODO, kary pieniężne nie mogą przekraczać kwoty przewidzianej za najcięższe naruszenie.

Załącznik nr 14 do Polityki Bezpieczeństwa – Nexpertis sp. z o.o.

PROCEDURA ochrony danych w fazie projektowania oraz domyślnej ochrony danych

(„privacy by design" oraz „privacy by default")

CEL PROCEDURY

Celem niniejszej procedury (DPIA) jest zapewnienie zgodności z wymogami wynikającymi z przepisów 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 (ogólne rozporządzenie o ochronie danych), zwanego dalej RODO w zakresie wymogu uwzględnienia ochrony danych w fazie projektowania oraz domyślnej ochrony danych. (privacy by design oraz privacy by default)

ZAKRES STOSOWANIA

1. Niniejsza procedura ma zastosowanie do wszystkich czynności i operacji przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.
2. Procedurą objęte są dane osobowe w rozumieniu art. 4 pkt 1 RODO.

POSTANOWIENIA OGÓLNE

1. Odpowiedzialnymi za prawidłową realizację procedury oceny ryzyka dla praw i wolności osób których dane dotyczą, jest Administrator oraz kierownicy projektów realizowanych w Nexpertis.

PRZEBIEG PROCEDURY

1. Ocena na etapie planowania
    a. Na etapie planowania należy zebrać informacje do oceny. W pierwszym kroku należy dokonać inwentaryzacji danych, które zgodnie z założeniem będą przetwarzane w procesie. W tym celu należy wypełnić arkusz nr 1 stanowiący załącznik do niniejszej procedury.
    b. Po wypełnieniu arkusza, należy go wraz z innymi dokumentami tj. umowy powierzenia przetwarzania danych osobowych, formularze, regulaminy, przekazać do konsultacji IOD.
    c. Jeśli Nexpertis występuje w roli procesora to inwentaryzacja ma na celu spełnienie wymogów względem administratora, o których mowa w art. 28 RODO. W tej sytuacji należy ustalić także zakres możliwych obowiązków względem administratora danych, uwzględniając:
        i. Charakter przetwarzania,
        ii. Faktyczne możliwości,
        iii. Dostępne informacje.
2. Na podstawie zebranych w arkuszu danych należy określić obowiązki prawne wynikające z przepisów RODO oraz innych aktów prawnych które będą miały zastosowanie. W tym celu należy dokonać interpretacji w oparciu o arkusz nr 2. Oceny dokonuje IOD lub osoba przez niego przeszkolona i wskazana. Dokumenty z inwentaryzacji i analizy przechowuje IOD.
3. W wyniku przeprowadzonej analizy prawnej obowiązków prawnych oraz rekomendowanych działań powinno doprowadzić do ustalenia akceptowalnego poziomu zgodności z przepisami ochrony danych osobowych i ryzyka w zakresie naruszenia zasad privacy by design oraz privacy by

Arkusz analizy - wskazówki dla IOD lub osoby upoważnionej do dokonania analizy

Lp.	Zagadnienia	Obowiązek prawny oraz /lub rekomendowane działanie
1.	Cel przetwarzania	Analiza czy do realizacji zakładanego celu niezbędnym jest zbieranie danych osobowych, czy cel przetwarzania jest zgodny z prawem. Zebranie informacji na temat założeń i charakteru akcji. Czy w zespole powołana zostanie osoba odpowiedzialna za ochronę danych osobowych
2.	Zakładana podstawa prawna przetwarzania danych osobowych	Sprawdzenie możliwości wystąpienia przesłanki określonej w art.6 RODO oraz jeśli podstawą przetwarzania będzie zgoda, przygotowanie odpowiedniej klauzuli wraz z wytycznymi co do sposobu jej zbierania.
3.	Opis kategorii osób, których dane będą przetwarzane	Informacja niezbędna do rejestru przetwarzania oraz oceny czy osobą której dane dotyczą może być dziecko, którego zgoda powinna być potwierdzona przez opiekuna prawnego. Informacja niezbędna do prowadzenia rejestru czynności przetwarzania.
4.	Zakładany zakres danych przetwarzanych w ramach procesu	Analiza adekwatności przetwarzania (minimalizacja danych) w związku ze znamy już celem przetwarzania danych. Informacja niezbędna do prowadzenia rejestru czynności przetwarzania.
5.	Szacowana maksymalna skala danych przetwarzanych w ramach projektu np.. 0-1000 rekordów, 1000-10000 rekordów itp.	Dana niezbędna do oszacowania skali przetwarzania.
6.	Wykaz podmiotów, który planowane jest zlecenie wykonania poszczególnych czynności w procesie, oraz inne podmioty współpracujące przy ustalaniu celów procesu przetwarzania.(należy wskazać nazwę podmiotu, adres oraz jego rolę)	Analiza i przygotowanie umów powierzenia oraz podpowierzenia. Ocena kontrahenta pod kątem wywiązywania się z zasad ochrony danych osobowych. Prowadzenie rejestru powierzeń, udostępnień wraz z analizą podstawy prawnej udostępnienia, analiza możliwości wystąpienia współadministrowania.
7.	W przypadku planowania współpracy z podmiotami wskazanymi powyżej, należy wskazać czy projekt umowy, bądź poprzednio zawarta umowa reguluje kwestie związane z powierzeniem przetwarzania danych osobowych, w szczególności czy cel i zakres wskazany w umowie odpowiada planowanemu (jeśli umowa została zawarta wcześniej należy wskazać do kiedy obowiązuje).	Analiza i przygotowanie umów powierzenia oraz podpowierzenia lub aneksów do umów już zawartych. Ocena kontrahenta pod kątem wywiązywania się z zasad ochrony danych osobowych.
8.	Podmiot lub Podmioty od który planowane jest pozyskanie bazy lub Pomiot lub Pomioty którym baza zostanie przekazana	Analiza podstawy prawnej nabycia/zbycia bazy
9.	Lista systemów informatycznych i teleinformatycznych, które będą wykorzystywane do realizacji procesu, oraz wskazanie przepływu danych między nimi (przypadku korzystania z podmiotów zewnętrznych np. przy usługach hostingowych należy podać nazwę i adres takiej firmy)	Lista niezbędna do przeprowadzenia sprawdzenia systemów IT oraz w razie takiej konieczności zawarcia umów powierzenia.
10.	Zakres danych przetwarzanych w poszczególnych systemach	Lista niezbędna do przeprowadzenia sprawdzenia systemów IT oraz ustalenia niezbędnych środków zabezpieczających dane osobowe.
11	Planowany czas trwania procesu, łącznie z archiwizacją danych oraz sposób usunięcia danych	Informacja niezbędna do prowadzenia rejestru czynności przetwarzania oraz wypełnienia obowiązków informacyjnych.
12.	Wykaz stron internetowych które będą wykorzystywane w procesie	Analiza źródeł zbierania danych pod kątem ich zabezpieczeń, przygotowanie klauzul obowiązków informacyjnych (wraz z wytycznymi co do ich zamieszczania) oraz konieczności przeprowadzenia privacy by default. Analiza postanowień regulaminów.
13.	Wykaz planowanych formularzy i innych dokumentów, które będą	Przygotowanie klauzul obowiązków informacyjnych (wraz z wytycznymi co do ich zamieszczania)