PRZYGOTUJ SIĘ DO RODO

ROZPORZĄDZENIE OGÓLNE OCHRONY DANYCH OSOBOWYCH

Praktyczny poradnik

make SOFT | usługi IT dla biznesu

make-SOFT Marcin Kazimierczak
ul. E. Estkowskiego 16/10, 66-400 Gorzów Wielkopolski
biuro@make-soft.pl
+48 691 185 359
www.make-soft.pl
/makesoft

Szanowni Państwo

25 maja 2018 wchodzą w życie wymagania nowego Rozporządzenia o Ochronie Danych Osobowych (RODO). Rozporządzenie dotyczy wszystkich organizacji przetwarzających dane osobowe (DO). Skupia się na uszczelnieniu ochrony i procedurach uruchamianych w przypadku utraty poufności danych. Zaostrzeniu uległy również kary za wyciek, wynoszące do 20 000 000 euro lub 4% światowego obrotu.

Podmiot i przedsiębiorcy, którzy w ramach swojej działalności przetwarzają dane osobowe – niezależnie od sektora gospodarki oraz wielkości i profilu prowadzonej działalności - będą mieli obowiązek wdrożenia i stosowania środków mających zapewnić bezpieczeństwo usług świadczonych przez Internet oraz prywatnych sieci i systemów informatycznych. Jednocześnie, od 25 maja 2018 roku podmioty te będą zobligowane do zgłaszania incydentów, w tym ataków hakerskich, mających niekorzystny wpływ na bezpieczeństwo przetwarzanych przez nich danych, właściwym organom, a także klientom, jeśli atak zagrozi ich danym osobowym bądź prywatności. Na tych, którzy nie zadbają należycie o bezpieczeństwo informacji o swoich klientach, będą nakładane bardzo surowe kary finansowe.

Nowe podejście do ochrony danych osobowych zakłada, że zakres obowiązków podmiotów przetwarzających dane osobowe będzie częściowo uzależniony od oceny ryzyka związanego z wykonywanymi przez podmiot czynnościami przetwarzania danych.

Jest to istotna nowość. Jeśli zatem przedsiębiorca lub organizacja przetwarza dane osobowe jedynie pomocniczo, np. w związku z zatrudnianiem swoich pracowników, to zakres wymagań regulacyjnych jaki będzie zobowiązany spełnić, będzie wyraźnie mniejszy, niż zakres obowiązków podmiotu, którego główna działalność polega na przetwarzaniu danych osobowych, np. agencji ubezpieczeniowych, sklepów internetowych, czy gabinetów medycznych. Nowością jednak przede wszystkim jest nie tylko deklaracji zgodności z określonymi zasadami, ale także zdolności jej wykazania.

W przygotowanym przez nas informatorze znajdziecie Państwo praktyczne informacje, które ułatwią wdrożenie RODO oraz pozwolą ocenić gotowość organizacji.

Z poważaniem,
Marcin Kazimierczak

Pełnił funkcję dyrektora obszaru IT w Urzędzie Miasta Gorzowa Wielkopolskiego.
Od 20 lat związany z obszarem utrzymania oraz rozwoju systemów teleinformatycznych. Specjalista w zakresie zarządzania usługami IT, organizacji ochrony informacji oraz rozwiązań Business Intelligence i integracji systemów teleinformatycznych. Tworzył dedykowane rozwiązania dziedzinowe oraz rozwiązania BI dla sektora bankowego oraz energetycznego.

make-SOFT Marcin Kazimierczak
ul. E. Estkowskiego 16/10, 66-400 Gorzów Wielkopolski
biuro@make-soft.pl +48 691 185 359
www.make-soft.pl /makesoft

Rewolucja w ochronie danych osobowych

Rozporządzenie ogólne o ochronie danych osobowych jest zmianą rewolucyjną, stawiającą nowe fundamenty dla systemu ochrony danych osobowych w Unii Europejskiej. To duże wyzwanie organizacyjne i finansowe. Na dostosowanie się do nowych regulacji przedsiębiorcy mają czas do 25 maja 2018 roku.

PRAWO PODMIOTU DANYCH
- rozbudowane prawo do informacji, prawo do bycia zapomnianym

ZGŁASZANIE INCYDENTÓW
- do 72 godzin, wysokie kary za brak zgłoszenia

KARY FINANSOWE
- do 20 mln euro lub 4% wartości rocznego obrotu

ZASIĘG GLOBALNY
- wszędzie tam, gdzie przetwarzane są dane osobowe obywateli EU

Nowe regulacje mają na celu stworzenie ram prawnych, w których zmieszczą się sieci społecznościowe, blockchain, Big Data, chmura obliczeniowa, technologie ubieralne, rozszerzona rzeczywistość, geolokalizacja i inne zjawiska społeczeństwa informacyjnego. Prawne uregulowanie nowych technologii przetwarzania danych, w tym takich, o których dziś nikt jeszcze nie pomyślał, a które za rok czy za dwa lata będą w powszechnym użyciu, wymaga stworzenia elastycznych przepisów, jakie będą nadążały za dynamiką świata IT. Z tego powodu Rozporządzenie nie wskazuje konkretnych rozwiązań technicznych czy organizacyjnych, które powinny zostać wdrożone, ale wymaga, aby te rozwiązania wypracował i wdrożył podmiot przetwarzający dane osobowe – odpowiednio do sytuacji.

Fundamentalnym pojęciem nowego europejskiego ładu ochrony danych osobowych jest ryzyko przetwarzania danych, które polega na prawdopodobieństwie naruszenia praw lub wolności osób fizycznych w toku przetwarzania dotyczących ich danych. To ryzyko w różnym stopniu dotyczy każdego, kto zbiera, modyfikuje, udostępnia, przechowuje, a nawet tylko usuwa dane, niezależnie od tego, czy robi to dla własnego celu, czy też wykonuje czynności zlecone przez inną osobę. Zgodnie z Rozporządzeniem podmioty przetwarzające dane będą musiały analizować procesy przetwarzania danych osobowych, w których uczestniczą, w kontekście ryzyk naruszenia praw i wolności osób fizycznych. Oceniając ryzyko,

make-SOFT Marcin Kazimierczak
ul. E. Estkowskiego 16/10, 66-400 Gorzów Wielkopolski
biuro@make-soft.pl +48 691 185 359
www.make-soft.pl /makesoft

będzie trzeba uwzględniać zakres danych, cel, kontekst i charakter przetwarzania. Wynik analizy będzie miał realny wpływ na zakres obowiązków regulacyjnych, będzie także podstawą do podjęcia decyzji o tym, jakie środki ochrony będą adekwatne do potencjalnych zagrożeń. Zgodnie z wytyczną *privacy by design*, wszystkie procesy przetwarzania będą musiały być projektowane (lub modyfikowane) tak aby zapewnić spełnienie wymagań Rozporządzenia ogólnego oraz minimalizować ryzyko związane z przetwarzaniem danych. Warto zwrócić uwagę, że przeprowadzenie analizy ryzyka związanego z przetwarzaniem danych będzie możliwe jedynie w warunkach, w których podmiot przetwarzający dane ma pełną świadomość procesów przetwarzania danych, których jest uczestnikiem.

Przed przystąpieniem do analizy trzeba będzie odpowiedzieć na pytania o zakres przetwarzania danych, jego cel i środki techniczne (w tym systemy informatyczne) wykorzystywane do przetwarzania. Bez udzielenia odpowiedzi na te podstawowe pytania wdrożenie wymagań Rozporządzenia ogólnego może okazać się niemożliwe.

Nowe podejście do ochrony danych osobowych zakłada, że zakres obowiązków podmiotów przetwarzających dane osobowe będzie częściowo uzależniony od oceny ryzyka związanego z wykonywanymi przez dany podmiot czynnościami przetwarzania danych. Jest to istotna nowość. Obecnie zakres obowiązków jest właściwie jednakowy dla wszystkich przetwarzających, co skutkuje nieadekwatnością wymagań regulacyjnych.

Z jednej strony istnieją podmioty, które przetwarzają niewielkie ilości danych, robiąc to jedynie pomocniczo w stosunku do swojej głównej działalności. Z drugiej strony mamy podmioty, które z przetwarzania danych uczyniły podstawę swoich usług, przetwarzając je na szeroką skalę. Stawianie jednym i drugim jednakowych wymagań musi skutkować przeregulowaniem działalności tych pierwszych lub niedoregulowaniem tych drugich. W konsekwencji część przedsiębiorców narzeka na nadmierne obciążenia i biurokrację, a przetwarzanie danych przez pozostałych wymyka się regulacjom prawnym (mamy nieefektywne prawo).

Rozporządzenie zmierza do zmiany tego stanu rzeczy. Zgodnie z nowymi przepisami zakres obowiązków regulacyjnych będzie pochodną oceny ryzyka związanego z przetwarzaniem danych przez określony podmiot przetwarzający.

Rozporządzenie ogólne o ochronie danych osobowych wymaga nie tylko zgodności działania z określonymi w nim zasadami, ale także zdolności wykazania tej zgodności. W praktyce oznacza to m.in., że podmioty przetwarzające dane będą musiały prowadzić dokumentację potwierdzającą spełnienie określonych w Rozporządzeniu wymagań. Nie chodzi jedynie o polityki, ale także o dokumentację procesów decyzyjnych, których następstwem jest określone działanie lub zaniechanie w obszarze ochrony danych osobowych. Przykładowo w przypadku decyzji o niewyznaczeniu inspektora ochrony danych podmiot przetwarzający powinien opracować i utrwalić dla celów dowodowych analizę wskazującą na brak obowiązku jego wyznaczenia. Nie wystarczy po prostu nie powołać. Z zasady rozliczalności wynika, że podmiot przetwarzający będzie musiał wykazać, że podjął decyzję o niepowoływaniu na podstawie analizy przepisów i własnej sytuacji faktycznej.

make-SOFT Marcin Kazimierczak
ul. E. Estkowskiego 16/10, 66-400 Gorzów Wielkopolski
biuro@make-soft.pl +48 691 185 359
www.make-soft.pl /makesoft

Jak rozumieć i stosować podejście oparte na ryzyku?

Ogólne rozporządzenie o ochronie danych (RODO) nie odnosi się wprost do procesu zarządzania ryzykiem i nie wskazuje konkretnej metody przeprowadzania oceny w tym zakresie. Każdy podmiot musi dokonywać jej samodzielnie, uwzględniając wiele specyficznych dla niego czynników, takich jak wielkość, struktura organizacyjna, możliwości techniczne czy zakres i rodzaj danych oraz cel ich przetwarzania.

Podejście oparte na ryzyku powoduje konieczność dokonywania oceny skutków następstw oraz prawdopodobieństwa wystąpienia zagrożeń utraty integralności, poufności lub dostępności. Należy również pamiętać, że dostosowanie organizacji do RODO nie jest jednorazowym działaniem ale procesem, w którym zaangażowana powinna być cała organizacja, a przyjęte zasady i procedury powinny być efektywne i zrozumiałe dla wszystkich.

Motyw 74 Preambuły:

Należy nałożyć na administratora obowiązki i ustanowić odpowiedzialność prawną administratora za przetwarzanie danych osobowych przez niego samego lub w jego imieniu. W szczególności administrator powinien mieć obowiązek wdrożenia odpowiednich i skutecznych środków oraz powinien być w stanie wykazać, że czynności przetwarzania są zgodne z niniejszym rozporządzeniem oraz, że są skuteczne. Środki te powinny uwzględniać charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych.

RODO przyjmuje podejście adekwatności – oznacza to, że drogi do osiągnięcia zgodności mogą być różne dla każdej firmy. Wymaga analizy istniejącego poziomu ryzyka oraz uzasadnienia, dlaczego wybrane metody zabezpieczeń są wystarczające.

Wdrożenie regulacji będzie szczególnie wymagające w przypadku dużych firm posiadających własne działy IT, które najczęściej posiadają własne zasoby IT, prawne oraz audytu. Niezależnie jednak od wielkości organizacji, celów przetwarzania danych osobowych oraz ich skali - zakres zastosowania odpowiednich i skutecznych środków będzie zawsze wynikał z analizy ryzyka, dla którego odniesieniem powinien być audyt obecnie stosowanych organizacyjnych i technicznych środków ochrony informacji.

Analizę ryzyka i dostosowanie modelu operacyjnego najlepiej przeprowadzić z wykorzystaniem normy ISO/IEC 27001:2013 – zarządzanie bezpieczeństwem informacji.

W zależności od oczekiwań klienta, możemy uczestniczyć przy wdrażaniu RODO jako **podmiot zarządzający projektem**, **doradca-ekspert poprzez hotline** lub **jako członek zespołu projektowego**.

Dopiero wdrożenie poaudytowych wniosków i zaleceń pozwoli stwierdzić że organizacja jest

RODO/GDPR *ready*

make-SOFT Marcin Kazimierczak
ul. E. Estkowskiego 16/10, 66-400 Gorzów Wielkopolski
biuro@make-soft.pl +48 691 185 359
www.make-soft.pl /makesoft

Wdrożenie RODO w organizacji – kluczowe działania

Dotychczas uzyskanie zgodności regulacyjnej w obszarze bezpieczeństwa sprowadzało się do zakupu „Polityki ochrony danych osobowych" i uzupełnienia rejestru danych. Obecnie, oprócz polityki (opisu wymagań) wymagane jest udokumentowanie procesów oraz zapewnienie dowodów, że są one realizowane.

Szablonowe rozwiązania, choć tańsze, długofalowo będą generować wyższe koszty utrzymania. W skrajnych przypadkach dodatkowe obowiązki mogą sparaliżować działanie przedsiębiorstwa. Z tego względu, organizacje potrzebują opracować własny system, dostosowany zarówno do potrzeb jak i posiadanych zasobów.

RODO wymusza na Administratorze Danych Osobowych badanie charakteru, zakresu, kontekstu i celów przetwarzania, co oznacza że problem ten dotyczy wszystkich komórek organizacyjnych, w których:

- dochodzi do przetwarzania danych osobowych (zachodzą realne procesy przetwarzania danych) oraz
- zapadają decyzje lub realizowane są czynności, które mogą mieć realny wpływ na procesy przetwarzania danych osobowych.

Skoro RODO wymaga, abyśmy uwzględnili zakres, kontekst i cele przetwarzania danych – to musimy być gotowi do ustalenia cyklu życia danych osobowych w ujęciu procesowym (czyli od momentu ich pozyskania, poprzez ich przetwarzanie w określonych celach i kontekstach biznesowych, aż po ich usunięcie).

Przykładem wymogu prawnego, który uzależniony jest między innymi od podstawy prawnej przetwarzania danych, którą stosujemy jest słynne już "prawo do bycia zapomnianym", a więc prawo żądania przez podmiot danych usunięcia jego danych osobowych przez Administratora. W praktyce z tego prawa osoby fizyczne będą mogły skorzystać głównie wówczas gdy Administrator danych przetwarzał ich dane na podstawie udzielonej zgody i zgoda ta została cofnięta przez podmiot danych. W takich wypadkach Administrator danych, o ile nie dysponuje inną podstawą prawną do przetwarzania danych, powinien je niezwłocznie usunąć. Powinien o potrzebie usunięcia danych powiadomić również inne podmioty, którym te dane ewentualnie udostępnił.

Jeżeli konkretna organizacja dokładnie wie, na jakich podstawach prawnych przetwarza dane osobowe w ramach poszczególnych celów i procesów biznesowych, bez problemu jest w stanie przewidzieć w jakich przypadkach podmiot danych może ewentualnie skorzystać z tego uprawnienia. Może więc oszacować ryzyko potrzeby spełnienia tego wymogu i zaplanować to w swoich procesach.

Dzięki temu spółki produkcyjne, które głównie przetwarzają dane osobowe kadrowe powinny sobie zdawać sprawę, że np. zatrudniani przez nie pracownicy mają bardzo ograniczoną (jeśli wręcz nie iluzoryczną) możliwość skorzystania z prawa do bycia zapomnianym - ponieważ ich pracodawca ma obowiązek przetwarzać ich dane osobowe w ramach stosunku zatrudnienia (prowadząc między innymi teczki osobowe).

make-SOFT Marcin Kazimierczak
ul. E. Estkowskiego 16/10, 66-400 Gorzów Wielkopolski
biuro@make-soft.pl +48 691 185 359
www.make-soft.pl /makesoft

Z kolei podmioty przetwarzające dane na dużą skalę **w celach marketingowych** muszą być świadome tego, że bazując na zgodzie jako podstawie prawnej przetwarzania danych są wysoce narażone na ryzyko stosowania "prawa do bycia zapomnianym".

Projekt wdrożenia RODO w organizacji

Wdrożenie wymagań RODO to proces **zarządzania zmianą** w organizacji. Na ile duża będzie to zmiana, zależy przede wszystkim od wyników przeprowadzonego audytu oraz podjętych decyzji odnośnie tego w jakim zakresie organizacja dostosuje się do wymagań ogólnego rozporządzenia o ochronie danych oraz za pomocą jakich środków i rozwiązań ten proces przeprowadzi.

Niewątpliwie zarówno ze względu na złożoność, czasochłonność oraz zaangażowanie zasadne jest wdrożenie RODO w oparciu o **metodykę zarządzania projektem**. Podejście projektowe jest skuteczną metodą realizacji planowanych działań oraz monitoringu projektu.

Powołanie struktury organizacyjnej

Bardzo rzadko zdarza się, aby wyłącznie jeden dział przetwarzał dane osobowe, dlatego wdrożenie RODO wymaga szerokiego zaangażowania, aby uwzględnić wszystkie obszary działalności biznesowej, zarówno front-end oraz back-office. Wynika to z innych perspektyw na zagadnienia związane z przetwarzaniem danych osobowych przez działy marketingu, kadr czy IT. Ostatecznie właśnie poszczególni pracownicy będą stosować rozwiązania zgodne z RODO, dlatego zarówno kontekst właścicieli procesów, ale również efektywnej realizacji procesów będzie kluczowy w projekcie.

Ważne, aby całość działań koordynował Kierownik Projektu, a za stworzenie dogodnych warunków do realizacji projektu, zapewnienie zasobów oraz nadzór odpowiadał Sponsor Projektu.

W przypadku powierzenia zarządzania projektem wdrożenia RODO, niezbędne będzie stopniowe przekształcenie Projektu w proces, w tym budowanie świadomości najwyższego kierownictwa – to Administrator Danych Osobowych odpowiedzialny jest za eksploatację i ewaluację systemu ochrony danych osobowych.

Faza przygotowawcza

W trakcie fazy przygotowawczej opracowany powinien zostać audyt RODO, z uwzględnieniem:

- analizy kontekstu organizacji,
- legalności przetwarzania danych (przesłanki legalności),
- przyjętych środków organizacyjnych i technicznych,
- obowiązków notyfikacyjnych do regulatora (incydenty, wyznaczenie inspektora ochrony danych),
- obowiązków informacyjnych i praw przysługujących osobom, których dane są przetwarzane,
- ocena świadomości osób przetwarzających dane osobowe,
- analizę ryzyka,

make-SOFT Marcin Kazimierczak
ul. E. Estkowskiego 16/10, 66-400 Gorzów Wielkopolski
biuro@make-soft.pl +48 691 185 359
www.make-soft.pl /makesoft

Kontekst organizacji, cele przetwarzania, analiza środków organizacyjnych i technicznych oraz analiza ryzyka powinny stanowić podstawę do opracowania planu niezbędnych działań związanych z dostosowaniem organizacji do RODO.

Przeprowadź analizę kontekstu organizacji oraz legalności przetwarzania danych

Dowiedz się, jakie dane osobowe są przetwarzane w Twojej organizacji oraz opisz ich przepływ od momentu pozyskania, aż do usunięcia. Uwzględnij procesy, systemy informatyczne i role osób odpowiedzialnych za ich przetwarzanie. Poniższych kilka pytań pomoże Ci uprościć sposób, w jaki przetwarzasz dane i obniżyć koszty na etapie wdrożenia:

- Jakie dane osobowe są w posiadaniu Twojej organizacji?
- Kto jest właścicielem danych?
- Jak i w jakim celu zostały pozyskane?
- Kto i w jaki sposób przetwarza te dane? Czy jesteś w stanie ograniczyć ilość tych lokalizacji?
- Czy istnieje potrzeba, aby je nadal przechowywać? Kiedy będzie można je usunąć?

Dokonaj oceny obowiązujących środków organizacyjnych i technicznych

Ocena środków organizacyjnych powinna zawierać analizę zgodności wymogów wynikających z rozporządzenia oraz przyjętych w organizacji zasad w zestawieniu z ustanowionymi procedurami postępowania. Oprócz oceny formalnej, należy dokonać kontroli merytorycznej.

Ocena środków technicznych powinna zostać zrealizowana poprzez kontrolę stosowania przyjętych zasad oraz analizę podatności systemów informatycznych.

Uzyskaj odpowiedzi na następujące pytania:

- Czy wszystkie osoby posiadające do nich dostęp na pewno go potrzebują?
- W jaki sposób są rejestrowane czynności związane z administrowaniem oraz działaniem systemów w których przetwarzane są dane osobowe?
- Udowodnić, że osoby przetwarzające dane posiadają upoważnienia do przetwarzania danych osobowych.
- Udowodnij, że fizyczne środki bezpieczeństwa zapewniają ochronę danych osobowych.
- Udowodnij, że stosowane są procedury rozliczalności administratorów systemów.
- Udowodnij, że uprawnienia dla użytkowników nadawane są z zachowaniem zasad minimalnych wymaganych uprawnień,
- Udowodnij stosowanie procedur zarządzania zmianą dla środowisk informatycznych, w tym dla środowisk produkcyjnych, rozwojowych i testowych?
- Udowodnij, że przechowujesz dane osobowe w sposób bezpieczny.
- Udowodnij, że osoby niepowołane nie uzyskają dostępu do urządzeń sieciowych.
- Udowodnij, że dokumenty są odpowiednio zabezpieczone.

Przeprowadź ocenę ryzyka utraty poufności, integralności oraz dostępności danych (ang. PIA). Zdolność pomiaru ryzyka jest kluczowym elementem zbudowania efektywnego systemu zabezpieczeń.

make-SOFT Marcin Kazimierczak
ul. E. Estkowskiego 16/10, 66-400 Gorzów Wielkopolski
biuro@make-soft.pl +48 691 185 359
www.make-soft.pl /makesoft

- Jakie konsekwencje dla poszkodowanych miałby wyciek danych, które przechowujesz (utrata poufności)?
- Jakie oddziaływanie będzie miała czasowa niedostępność systemów/danych (utrata dostępności)?
- Jakie oddziaływanie będzie miała zmiana/utrata danych (utrata integralności danych)?
- Kto powinien, a kto ma dostęp do danych (nadawanie i odbieranie uprawnień)?
- Czy przeprowadzana jest procedura przywracania danych z kopii bezpieczeństwa?
- Czy opracowany jest Plan Ciągłości Działania dla środowisk produkcyjnych?
- Czy zarządzanie systemem informatycznym odbywa się z uwzględnieniem rozliczalności procesów?
- Czy na jakimkolwiek etapie przetwarzania, udostępniasz je zewnętrznym dostawcom?

Faza realizacyjna

Ten etap wymaga wdrożenia zaleceń oraz podjęcie działań w celu zapewnienia zgodności z rozporządzeniem. Bardzo często wymagane jest zaangażowanie sporych nakładów, aby w sposób prawidłowy i efektywny wzmocnić bezpieczeństwo danych. Na tym etapie należy również podjąć działania aby dostosować infrastrukturę informatyczną i eksploatowane systemy do wymogów RODO lub do osiągnięcia pożądanego poziomu bezpieczeństwa.

Wybierz rozwiązania adekwatne do potrzeb. Z czasem prawdopodobnie ukształtują się standardy dla poszczególnych branż. Do tego czasu najlepszym wyjściem będzie uzasadnienie swojego wyboru odniesieniem do „dobrych praktyk". Dwa lata temu sektor finansowy stał przed podobnym wyzwaniem, wdrażając zalecenia Rekomendacji D.

Opracuj polityki i standardy zawierające wymagania obowiązujące wszystkich pracowników organizacji. W kontekście RODO będziesz potrzebował zrewidować swoją dotychczasową Politykę Bezpieczeństwa Informacji (PBI) oraz dokumenty podrzędne.

Oto kilka wskazówek, które mogą być Ci pomocne na tym etapie:

- Opracuj nadrzędną politykę ze szczegółowymi standardami w formie załączników. Pomaga to uporządkować wiedzę i ograniczyć ilości informacji przekazywanych pracownikom, aby łatwiej mogli je przyswoić.
- Wytyczne bezpieczeństwa dla zewnętrznych dostawców sformułuj w postaci załącznika do umów.
- Opracuj przejrzysty standard klasyfikacji i ochrony informacji. Będzie to dokument przekazywany wszystkim pracownikom, zawierający wytyczne jak obchodzić się z poszczególnymi grupami informacji. Nieznajomość lub brak zrozumienia tych zasad jest bardzo częstą przyczyną wycieków.
- Zwróć uwagę na bezpieczeństwo urządzeń mobilnych. Wszystkie mobilne nośniki pamięci, na których zapisane są dane osobowe powinny być szyfrowane. Zapewnisz w ten sposób większą ochronę swoim klientom, jak również unikniesz kary w przypadku utraty nośnika.

make-SOFT Marcin Kazimierczak
ul. E. Estkowskiego 16/10, 66-400 Gorzów Wielkopolski
biuro@make-soft.pl +48 691 185 359
www.make-soft.pl /makesoft

Zwróć uwagę na następujące zagadnienia:

- Uwzględnienie bezpieczeństwa i prywatności na etapie projektowania rozwiązań.
- Wytyczne dotyczące złożoności haseł, częstotliwości ich zmian i sposobów zapisywania.
- Wytyczne dotyczące konfiguracji urządzeń sieciowych i stacji roboczych.
- Konieczność zapewnienia odpowiedniego poziomu ochrony danych osobowych przez dostawców usług.
- Wytyczne dotyczące pracy użytkowników z minimalnymi potrzebnymi uprawnieniami,
- Dopuszczalne sposoby przechowywania danych osobowych i wytyczne odnośnie ich zabezpieczeń.

Udokumentuj procesy i procedury opisujące poszczególne aktywności. Ogranicz ich poziom szczegółowości do niezbędnego minimum i stosuj ujednoliconą strukturę. Każdy proces powinien mieć wyznaczonego właściciela, odpowiedzialnego za jego utrzymanie i rozwój. Wykorzystuj kreatywność i doświadczenie swoich pracowników, aby doskonalić procedury – odstępstwa od przyjętych w politykach zasad powinny być jednak akceptowane przez właściciela.

Z perspektywy RODO najważniejsze są następujące procesy:

- Zarządzanie zgodami,
- Zarządzanie dostępem do systemów informatycznych w których przetwarzane są dane osobowe,
- Obsługa zgłoszeń klientów (prośba o udostepnienie lub usunięcie danych),
- Zarządzanie nośnikami pamięci zawierającymi dane osobowe,
- Zarządzanie incydentami bezpieczeństwa (monitorowanie, obsługa, powiadamianie o ich wystąpieniu, reagowanie),
- Edukacja pracowników i budowanie kultury bezpieczeństwa,
- Zarządzanie środowiskami nieprodukcyjnymi,

Oprogramowanie. Każda firma przetwarzająca dane osobowe niezależnie od skali, powinna posiadać system antywirusowy i firewall. Większe organizacje powinny rozważyć wdrożenie oprogramowania typu DLP (ochrona przed wyciekiem danych) oraz IPS (zapobieganie włamaniom). Przy zakupie oprogramowania warto skorzystać z pomocy niezależnego eksperta, który pomoże wybrać odpowiednie narzędzia i dostawcę.

Dla rozwiązań dziedzinowych, wspierających procesy biznesowe należy uwzględnić wdrażanie zasad „*privacy by design*" oraz „*privacy by default*", oznaczające konieczność obowiązku uwzględnienia ochrony danych i prywatności na każdym etapie tworzenia oraz istnienia technologii obejmującej ich przetwarzanie.

Jeśli świadczysz usługi dla podmiotów fizycznych poprzez usługi on-line (np. sklep internetowy, newsletter, email marketing), ustawienia aplikacji czy systemów przetwarzających dane domyślnie powinny gromadzić minimalną ilość informacji o użytkowniku. Poszerzenie zakresu gromadzonych i udostępnianych danych może nastąpić jedynie na podstawie zmiany ustawień dokonanych przez samego

make-SOFT Marcin Kazimierczak
ul. E. Estkowskiego 16/10, 66-400 Gorzów Wielkopolski
biuro@make-soft.pl +48 691 185 359
www.make-soft.pl /makesoft

użytkownika. Nie zapomnij o poinformowaniu w polityce prywatności o celach przetwarzania danych, jakie informacje zbierasz i/lub jakiem usługodawcom/podmiotom powierzasz przetwarzanie danych (hosting, analityka odwiedzin, remarketing).

Korzystanie z usług zgodnych z RODO

Jeśli korzystasz z oprogramowania w modelu SaaS (ang. Software-as-a-Service), musi być zawarta umowa powierzenia przetwarzania danych osobowych oraz zapewnienie o zgodności z RODO. Dotyczy to np. usług backupu, hostingu, Email Marketing Automation, sklepu internetowego. Również umowy utrzymaniowe systemów teleinformatycznych, jeśli świadczone są przez osoby trzecie, muszą zawierać odpowiednie klauzule dotyczące poufności i ochrony danych osobowych. Jako administrator danych osobowych masz również prawo żądać udowodnienia, że procesor wypełnił wymagania związane ze zgodnością z rozporządzeniem ochrony danych osobowych. Przygotowywany nowy projekt ustawy krajowej o ochronie danych osobowych wprowadzi możliwość certyfikowania podmiotów przetwarzających dane, co w konsekwencji doprowadzi do możliwości weryfikacji podmiotów posiadające certyfikat będą z pewnością mogły być traktowane jako zaufane zapewniające pełną zgodność z RODO.

Utworzenie roli Inspektora Ochrony Danych. Głównymi obowiązkami tej osoby jest koordynowanie procesów odpowiadających bezpośrednio za bezpieczeństwo, oraz zarządzanie ryzykiem cybernetycznym. Inspektor powinien bardzo dobrze znać wymagania regulacyjne oraz architekturę lokalnego systemu bezpieczeństwa. Powinien być w stanie uzasadnić adekwatność wybranych rozwiązań, oraz dostarczyć dowodów poświadczających, że system działa zgodnie z założeniami.

Szkolenia i programy budowania świadomości. Duży nacisk, jaki RODO kładzie na edukację, świadczy o strategicznym podejściu mającym zachęcić firmy do tego, aby myślały o bezpieczeństwie w bardziej kompleksowy sposób. Podstawowym narzędziem podnoszącym świadomość użytkowników jest przeprowadzanie szkoleń, powtarzanym cykliczne w celu zbudowania właściwych nawyków. Dodatkowo, w przypadku stanowisk szczególnie podatnych na ataki, zaleca się zapewnienie pracownikom dedykowanych szkoleń.

> Pamiętaj,
> najsłabszym ogniwem systemów bezpieczeństwa informacji
> – jest człowiek!

Zarządzanie ryzykiem, pomiar metryk bezpieczeństwa i gromadzenie dowodów. „Bezpieczeństwo" jest procesem, nie projektem. Rozwiązania, które zostaną opracowane na etapie wdrożenia, będzie trzeba monitorować i świadomie rozwijać. Większe projekty, nowi dostawcy usług i zakup oprogramowania będą wymagały weryfikacji, czy zapewniają zgodność z wymaganiami zawartymi w Polityce Bezpieczeństwa Informacji. Trzeba również pamiętać, że zapewnienia bezpieczeństwa systemów teleinformatycznych jest w dużej mierze nieosiągalne, dlatego należy poprawiać i reagować.

make-SOFT Marcin Kazimierczak
ul. E. Estkowskiego 16/10, 66-400 Gorzów Wielkopolski
biuro@make-soft.pl +48 691 185 359
www.make-soft.pl /makesoft

Podsumowanie

Rozporządzenie w sposób znaczący zmienia podejście do bezpieczeństwa danych osobowych oraz prywatności osób fizycznych. Mając na względzie zagadnienia związane z bezpieczeństwem informacji, wdrażanie systemu zabezpieczeń niewątpliwie zbieżne i w wielu aspektach jest z systemami zarządzania opartymi na cyklu PDCA (ang. Plan-Do-Chekt-Act) Deminge'a. Biorąc pod uwagę, że organizacje i tak muszą dostosować swoje procesy, procedury, zarządzać ryzykiem, czy przyjąć polityki bezpieczeństwa dla danych osobowych, wskazane jest rozważenie ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), zawierającego wiele wspólnych elementów, m.in. inwentaryzację aktywów informacyjnych, ich klasyfikację, zarządzanie ryzykiem, opracowanie planu ciągłości działania, w stosunku do wszystkich zasobów informacyjnych. Jest to o tyle wskazane, że znaczną część działań i tak należy wykonać w związku z RODO, a zasoby informacyjne zawierające dane osobowe są szczególnym przypadkiem informacji wykorzystywanych w działalności biznesowej.

Zapewnienie zgodności z rozporządzeniem o ochronie danych osobowych jest wyzwaniem dla każdej organizacji, niezależnie od wielkości, sektora oraz struktury organizacyjnej, wymagającej zaangażowania wewnątrz organizacji, ale również wiedzy i doświadczenia z zakresu architektury korporacyjnej, prawnej oraz informatycznej.

make-SOFT Marcin Kazimierczak
ul. E. Estkowskiego 16/10, 66-400 Gorzów Wielkopolski
biuro@make-soft.pl
+48 691 185 359
www.make-soft.pl
/makesoft