GRUPA AF®

Audyt zgodności i wdrożenie RODO

GRUPA AF®

Audyt zgodności i wdrożenie RODO
Oferta bezkosztowa z odpisem PFRON

25 maja 2018r. zacznie obowiązywać 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 (ogólne rozporządzenie o ochronie danych – w skrócie **RODO**).

Pojawi się m.in. obowiązek powołania Inspektora Ochrony Danych i jego nowe zadania (np. zgłaszanie naruszeń w ciągu 72 godzin od wykrycia), nowe klauzule informacyjne i oceny ryzyka, ograniczenie profilowania, obowiązkowa inwentaryzacja danych - jednocześnie niedopilnowanie nowych obowiązków dotyczących ochrony danych osobowych może kosztować firmę nawet do **20 mln euro lub 4 proc. rocznego obrotu firmy** - w zależności od tego, która kwota jest wyższa. Nie bez znaczenia będzie także większa odpowiedzialność odszkodowawcza i cywilna właścicieli / zarządów firm.

Ochrona danych osobowych nie będzie zatem sprowadzała się do wykonania kilku jasno określonych czynności, a raczej zaprojektowania całego systemu tej ochrony – i ustawiania procedur osobno pod wszystkie procesy, jakie dzieją się w firmie i uwzględniają wykorzystanie danych osobowych.

Cel działania

Zbadanie zgodności działania klienta z wymogami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 679 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 - RODO).

Przygotowanie Organizacji do stosowania RODO poprzez wdrożenie systemu ochrony danych osobowych.. Aktualizacja wewnętrznych regulaminów pracowniczych zgodnie ze zmianami wynikającymi z zaprojektowanych przepisach sektorowych.

Zakres usługi

1. Audyt procesów przetwarzania danych osobowych;
2. Opracowanie metodyki Analizy ryzyka i Polityki zarządzania ryzykiem w obszarze ochrony danych osobowych;
3. Aktualizacja i uzupełnienie systemu ochrony danych osobowych, ze szczególnym uwzględnieniem polityki bezpieczeństwa;
4. Szkolenie dla pracowników z zasad przetwarzania i ochrony danych osobowych;
5. Wsparcie i doradztwo powdrożeniowe.

GRUPA AF®

Ad. 1

Audyt procesów przetwarzania danych osobowych:

a) Inwentaryzacja zbiorów i czynności przetwarzania danych w jednostce organizacyjnej:

- ustalenie rodzajów zbiorów danych klientów, pracowników czy danych powierzonych przez inne podmioty oraz celu ich przetwarzania,
- określenie statutu prawnego przetwarzanych danych,
- analiza procesów przetwarzania, w tym zbierania danych oraz ewentualnego profilowania osób lub szczególnych operacji przetwarzania, wymagających przeprowadzenia oceny skutków dla ochrony danych,
- analiza procesów przetwarzania, ze szczególnym uwzględnieniem danych osobowych gromadzonych na podstawie szczególnych przepisów prawa;

b) Analiza wypełnienia wymagań przepisów prawa (zarówno przepisów o ochronie danych osobowych, jak i przepisów sektorowych związanych z przetwarzaniem danych):

- analiza przesłanek legalności (podstaw prawnych), na podstawie których przetwarzane są dane osobowe,
- analiza realizacji obowiązku informacyjnego, w tym poprawności klauzul informacyjnych i oświadczeń na formularzach do zbierania danych osobowych,
- zbadanie realizacji obowiązków dotyczących celowości, adekwatności i czasu przetwarzania danych osobowych,
- analiza procedur dotyczących udostępniania danych innym podmiotom, w tym udostępniania danych do państw trzecich – poza UE,
- analiza umów związanych z powierzaniem danych innym podmiotom lub przez inny podmiot, ocena wypełnienia związanych z tym obowiązków,
- badanie realizacji praw osób, których dane są przetwarzane;

c) Ocena wypełnienia obowiązków technicznych i organizacyjnych:

- ocena przyjętej dokumentacji opisującej sposób przetwarzania danych,
- ocena prawidłowości zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych,
- ocena mechanizmów rozliczalności w aplikacjach przetwarzających dane osobowe;
- ocena realizacji zabezpieczenia systemu informatycznego i obszaru przetwarzania danych,
- ocena realizacji działań dotyczących nadawania upoważnień do przetwarzania danych osobowych oraz prowadzenia ewidencji osób upoważnionych,
- ocena wykonywania czynności nadzoru nad przetwarzaniem danych – analiza obowiązku wyznaczenia inspektora ochrony danych zgodnie z RODO,
- ocena sposobu realizacji wynikających z RODO praw osób, których dane osobowe dotyczą (prawo dostępu do danych; do sprostowania danych; ograniczenia przetwarzania; usunięcia danych; do ograniczenia przetwarzania; przenoszenia danych; sprzeciwu),

d) Przygotowanie raportu zawierającego:

- weryfikację procesów oraz obszarów przetwarzania danych osobowych,
- ocenę adekwatności stosowanych dotychczas zabezpieczeń technicznych i organizacyjnych,
- spis zaleceń mających na celu uporządkowanie procesów przetwarzania danych.

e) Spotkanie szkoleniowo-konsultacyjne dla kadry kierowniczej z przedstawieniem i analizą takich tematów jak:

- obecne i przyszłe obowiązki administratorów danych, w świetle zmienianych przepisów prawa. Zasady przetwarzania i współadministrowania danymi osobowymi w Grupie przedsiębiorstw.;
- nowe obowiązki informacyjne administratora;
- nowe prawa osób, których dane dotyczą;
- nowy zakres odpowiedzialności za przetwarzanie danych niezgodnie z przepisami;
- konieczne działania organizacyjne, prawne, techniczne, jakie należy podjąć, aby przygotować się do stosowania RODO – rozporządzenia ogólnego o ochronie danych osobowych

Ad. 2

Przeprowadzenie analizy ryzyka przetwarzania danych osobowych:

a) Wstępna identyfikacja zagrożeń dla praw i wolności osób, których dane są przetwarzane;

b) Przygotowanie arkusza analizy ryzyka;

c) Przeprowadzenie analizy ryzyka procesów realizowanych w każdej komórce organizacyjnej pod kątem przetwarzania danych osobowych oraz identyfikacja aktywów w nich wykorzystywanych i ryzyk naruszenia praw i wolności osób, a także wskazanie zabezpieczeń wdrożonych i potencjalnych, zmniejszających ryzyko;

d) Wyliczenie i ocena ryzyk oraz stworzenie listy (mapy) ryzyk;

e) Przygotowanie propozycji Planu postępowania z ryzykiem.

Ad. 3

3. Aktualizacja i uzupełnienie systemu ochrony danych osobowych:

a) Opracowanie projektów dokumentów dotyczących przetwarzania danych lub doprowadzenie do zgodności z wymogami przepisów prawa:

- polityki bezpieczeństwa,
- instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych, rejestru czynności przetwarzania danych osobowych, w tym – gdy będzie to adekwatne – rejestru wszystkich kategorii czynności przetwarzania dokonywanych przez podmiot przetwarzający w imieniu administratora,
- metodyki analizy ryzyka,
- procedury zgłaszania oraz postępowania w przypadku naruszeń ochrony danych,
- procedury realizacji praw osób, których dane dotyczą;

b) Opracowanie wzorów klauzul obowiązku informacyjnego i klauzul wyrażenia zgody, z uwzględnieniem wymagań RODO oraz innych przepisów prawa;

c) Opracowanie wzorów zapisów i wskazówek do uzupełniania umów powierzenia przetwarzania danych osobowych, z uwzględnieniem wymagań RODO;

d) Optymalizacja procesów przetwarzania danych i zabezpieczeń organizacyjnych;

e) Konsultacje przy zatwierdzaniu Planu postępowania z ryzykiem w zakresie określenia adekwatnych środków organizacyjnych i technicznych ;

f) Konsultacje i wsparcie we wdrażaniu wszystkich działań doskonalących.

Ad. 4

Szkolenie dla pracowników, a w szczególności dla osób upoważnionych do przetwarzania danych osobowych, z praktycznych aspektów ochrony danych:

a) Ochrona danych osobowych – aspekty prawne

- Zmiany w przepisach – RODO – rewolucja czy ewolucja
- Źródła prawa ochrony danych osobowych w Polsce
- Przepisy szczególne, m. in. Prawo pracy
- Podstawowe pojęcia
- Nowe pojęcia w RODO

b) Obowiązki związane z przetwarzaniem danych osobowych

- Prawa osób, których dane dotyczą
- Odpowiedzialność za naruszenie ochrony danych osobowych
- Przykłady naruszeń
- Dotkliwość kar

c) Ochrona danych osobowych - aspekty techniczno-organizacyjne

- ABI a IOD
- Przykłady zabezpieczeń
- Dokumentacja

d) Pytania

e) Podsumowanie

Ad. 5

Doradztwo powdrożeniowe – zdalnie (dokładny zakres do ustalenia):

a) Dostępność za pośrednictwem środków telekomunikacyjnych (email, telefon) dla koordynatora ds. ochrony danych wyznaczonego przez Zleceniodawcę przez okres dwóch miesięcy od zakończenia usługi;

GRUPA AF®

Warunki realizacji usług

Przebieg prac przy realizacji usług

Prace realizowane w ramach projektu będą prowadzone z uwzględnieniem potrzeb biznesowych Zamawiającego.

Usługa wykonana będzie przez osobę lub osoby mające wiedzę i doświadczenie adekwatne do złożoności usług.

Zakłada się wykonanie usługi w siedzibie Zleceniodawcy w terminie określonym w umowie, przy stałym współudziale wybranych osób dopuszczonych do przetwarzania danych osobowych (np. administrator bezpieczeństwa informacji, wyznaczeni przedstawiciele komórek organizacyjnych oraz administrator systemów informatycznych).

Nie wyklucza się wykorzystania we współpracy, w zależności od bieżących potrzeb, innych osób dopuszczonych do przetwarzania danych.

Poprawność merytoryczna wykonania usługi uzależniona jest od dostępu do informacji i udzielonych wyjaśnień.

Forma

1. Wyniki prac będą odbierane przez Zamawiającego w formie przyjętej po obopólnych ustaleniach Stron.
2. Wynikiem prac wdrożeniowych będzie kompleksowa dokumentacja z zakresu danych osobowych przekazana w formie elektronicznej, opracowana zgodnie z przepisami prawa z zakresu ochrony danych osobowych, z wykorzystaniem i w oparciu o normy ISO z grupy 27000.
3. Zamawiający otrzyma zaświadczenie o przejściu audytu z zakresu ochrony danych osobowych oraz wdrożeniu systemu ochrony danych osobowych zapewniającym zgodność przetwarzania i ochrony danych z obowiązującymi przepisami prawa, w szczególności z RODO - ogólnym rozporządzeniem o ochronie danych.

GRUPA AF®

Jak to działa?

- Oferujemy wykonanie audytu z odpisem Pfron wysokość ulgi 100%
- Przedsiębiorstwa zatrudniające powyżej dwudziestu pięciu pracowników płacą składki do PFRON (Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych) jeżeli zatrudniają mniej jak 6% osób niepełnosprawnych.
- Dla przykładu przedsiębiorstwo, które zatrudnia 100 osób musi zatrudnić 6 niepełnosprawnych pracowników, wówczas nie zapłaci kary. W przypadku kiedy nie zatrudnia osób niepełnosprawnych płaci co miesiąc ok. 10 tyś. zł na rzecz PFRON czyli rocznie 120 tyś. zł.
- 50% wyżej wymienionej kwoty przedsiębiorstwo może wydać kupując w GrupaAF usługi (wykonanie audytu i wdrożenia RODO), drugie 50% i tak należy wpłacić do PFRON zgodnie z ustawą o Rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych Artykuł 22, pkt.3.
- **Przedsiębiorstwo nadal wydaje 120 tyś. zł, ale dostaje usługi warte 60 tyś. zł. i fakturę VAT.**

Nasi Klienci

KGHM POLSKA MIEDŹ, GRYCAN, 4F, Mostostal Siedlce, TUI, PSB Polskie Składy Budowlane, Instytut Fizyki Polskiej Akademii Nauk, LUXOFT, ENERGOP, sefako, opec, KRAKBAU, multiMedia, DRAGADOS, asseco BUSINESS SOLUTIONS, MPK Legnica, BANIMEX, ADAMPOL SA, ITE, FineAltech, Italian Fashion

Referencje

GRUPA AF®

Nasi Eksperci

Michał Mrówka

Prawnik, prezes zarządu ODO Consulting. Audytem w obszarze ochrony danych osobowych zajmuje się od 6 lat. Doświadczony Administrator Bezpieczeństwa Informacji legitymujący się bogatym doświadczeniem w pełnieniu tej funkcji zarówno w podmiotach z sektora publicznego, jak i prywatnego. Certyfikowany audytor wewnętrzny normy ISO 27001. Członek Stowarzyszenia Inspektorów Ochrony Danych Osobowych. Autor opracowań dotyczących tematyki ochrony danych osobowych oraz ekspert w zakresie tematyki związanej z udostępnianiem informacji publicznej oraz cyberbezpieczeństwem.

Marcin Soczko

Certyfikowany audytor systemów zarządzania jakością ISO 9001 i zarządzania bezpieczeństwem informacji ISO 27001, członek zarządu Stowarzyszenia Administratorów Bezpieczeństwa Informacji. Brał udział w ponad 70 audytach i przeszkolił ponad 2000 osób. Wspierał organizacje w opracowaniu i wdrożeniu systemu ochrony danych osobowych lub systemu zarządzania bezpieczeństwem informacji. Pełni rolę ABI w kilku różnych organizacjach. Współautor publikacji i książek poruszających tematykę ochrony danych osobowych, m.in. Vademecum ABI. Część II – Przygotowanie do roli Inspektora Ochrony Danych.

Piotr Glen

Ekspert z wieloletnim doświadczeniem w stosowaniu prawa ochrony danych osobowych oraz wdrażaniu polityki bezpieczeństwa informacji w różnego rodzaju firmach i instytucjach. Członek Stowarzyszenia Administratorów Bezpieczeństwa Informacji SABI. Członek zespołów roboczych analizujących projekt nowej ustawy o ochronie danych osobowych. Certyfikowany audytor systemów zarządzania bezpieczeństwem informacji. Autor wielu książek i publikacji w zakresie ochrony danych osobowych. Trener i wykładowca - wysoko ceniony za praktyczne podejście do zagadnień ochrony informacji i stosowania przepisów prawa w tym zakresie.

Karolina Paluszek

Doktor nauk prawnych, doświadczony wykładowca akademicki, prawnik praktyk. Prowadzi badania naukowe w obszarze interpretacji prawa Unii Europejskiej, dokonywanej przez Trybunał Sprawiedliwości. Zajmuje się również zagadnieniami związanymi ze stosowaniem prawa ochrony danych osobowych oraz polityki bezpieczeństwa informacji w różnego rodzaju firmach i instytucjach. Laureatka Prestiżowego Konkursu Lady D w 2011 roku.

GRUPA AF®

Partner merytoryczny

Gawronski & Partners

Gawronski & Partners jest niezależną polską firmą prawniczą o szerokim obszarze doradztwa prawnego i wsparcia konsultingowego dla biznesu. Doradztwo m.in. w zakresie przetwarzania, powierzania, przenoszenia i międzynarodowych transferów danych osobowych, cloud computingu, cyberbezpieczeństwa, wdrażania Ogólnego Rozporządzenia UE o Ochronie Danych Osobowych (RODO), przygotowania do Rozporządzenia ePrivacy. Specjaliści kancelarii byli doradcami Komisji Europejskiej i unijnych regulatorów ochrony danych osobowych (Grupy Roboczej Art. 29).

Maciej Schab
Customer Service Director
(+48) 530 264 429
m.schab@GrupaAF.pl