Inspektor ds. ochrony danych osobowych na gruncie Rozporządzenia Parlamentu i Rady – model docelowy

Agnieszka Ferens-Sosnowska

„Przedsiębiorcy sami zdecydują jak właściwie chronić dane”

„ABI, jako strażnik przestrzegania przepisów o ochronie danych”

„Szczęśliwy ABI”

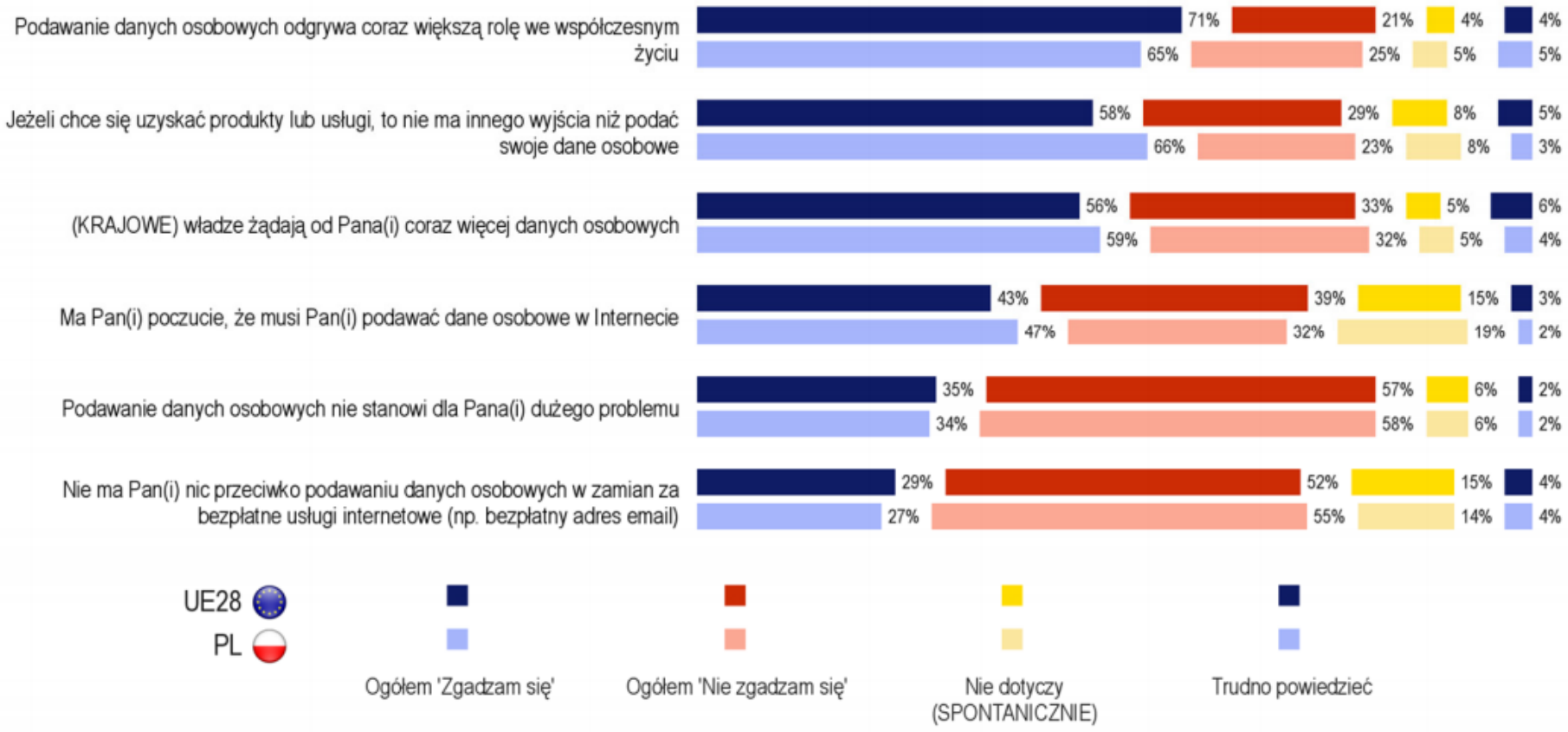
„Unijna reforma to szansa na lepszą ochronę danych”

„Nowa rola ABI”

„Administrator bezpieczeństwa informacji powinien być jak inspektor”

2. STOSUNEK DO UJAWNIANIA DANYCH OSOBOWYCH

W odniesieniu do każdego z następujących stwierdzeń, proszę powiedzieć, czy zgadza się Pan(i) z nim czy też nie zgadza.



Poprzednicy
Biuro
Statystyki i sprawozdania
Sprawozdania roczne
Statystyki
BIP

Serwisy GIODO
eduGIODO
e-GIODO

Rodzaj działalności			Okres (rok)				
			2011	2012	2013	2014	2015
Skierowane do GIODO	pytania z prośbą o interpretacje		3935	4258	4911	4575	2631
	skargi		1272	1593	1879	2472	1291
	akty prawne		603	656	617	561	375
Przeprowadzone kontrole			199	165	173	175	129
DECYZJE GIODO							
	Departament Edukacji Społecznej i Współpracy Międzynarodowej		50	51	134	97	41
	Departament Orzecznictwa, Legislacji i Skarg		539	762	646	548	390
	Departament Inspekcji		104	57	74	86	41
	Departament Rejestracji Zbiorów Danych Osobowych	o odmowie rejestracji	105	427	504	487	188
		umarzające postępowanie rejestracyjne	45				
		o wykreśleniu z ogólnokrajowego rejestru zbiorów danych osobowych	268				
	ogółem		1111	1297	1358	1218	461
Zawiadomienia o przestępstwie			9	12	16	10	15
Zbiory	zgłoszone do rejestracji		15643	21580	28264	43300	23376

GIODO pozytywnie o nowych instrumentach ochrony prywatności, 4.11.2015 r.
GIODO zawarł porozumienie o współpracy z Uniwersytetem Warszawskim, 5.11.2015 r.
Naruszający zasady ochrony danych osobowych nie będą bezkarni, 31.10.2015 r.
Szpital musi chronić informacje dotyczące pacjentów, 30.10.2015 r.
37. Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności

Ważne

Zasady przekazywania danych osobowych na terytorium USA
Przepisy o ochronie danych osobowych a marketing bezpośredni-debata, 27.10.2015 r.
Działalność służb specjalnych państwa a ochrona danych

Badania przeprowadzone przez Ponemon Institute „The bilion dolar lost laptop problem” wskazują, iż pracownicy różnych firm amerykańskich zgubili w roku 2010 ponad 85 tysięcy komputerów przenośnych. Z czego:

- Ponad połowa zagubionego sprzętu zawierała dane poufne
- Tylko 30% z nich miało szyfrowane dyski
- Tylko 10% posiadało inne zabezpieczenia
- 29% komputerów miało kopie zapasowe

Koszt?

- 2 miliardy dolarów
- Złamane kariery
- Utracona reputacja firmy
- Koszty sądowe oraz koszty związane z profesjonalnym zabezpieczeniem śladów

Według raportu stowarzyszenia ISACA z marca 2012 r.

- prawo jazdy – 147 euro
- dane bilingowe – 78- 294 euro
- świadectwo urodzenia – 147 euro

Frag. okładki książki „Tylnymi drzwiami. Czarny Rynek w PRL-u" Jerzy Kochanowski

Międzynarodowe badanie przygotowane przez firmę doradczą PwC, magazyn CIO oraz magazyn CSO „The Global State of Information Security Survey 2013” w którym przebadano około 9300 managerów ze 128 krajów pokazały, że tylko 40% managerów potrafi wskazać miejsce przechowywania wrażliwych informacji o klientach i pracownikach, a tylko 1/3 interesuje się jak zabezpieczone są dane przekazywane podwykonawcom.

Według ankietowanych barierą w poprawie bezpieczeństwa jest brak zaangażowania po stronie kierownictwa firmy oraz brak wykwalifikowanych pracowników.

„Jeśli przetwarzanie odbywa się w sektorze publicznym lub jeśli przetwarzanie w sektorze prywatnym prowadzi duże przedsiębiorstwo, lub jeśli główna działalność przedsiębiorstwa, niezależnie od jego wielkości, obejmuje operacje przetwarzania, które wymagają regularnego i systematycznego monitorowania, osoba trzecia powinna wspomagać administratora lub podmiot przetwarzający w monitorowaniu zgodności, na poziomie wewnętrznym, z niniejszym rozporządzeniem (...)".

Motyw 75 rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych)

Inspektor Ochrony Danych- „Dyrygent zgodności”

„Kluczowe tematy z perspektywy trilogu”

Grupa robocza art. 29 –„*Inspektor Ochrony Danych (Data Protection Officer) jest kluczowym elementem rozliczalności oraz realnym narzędziem konkurencyjności dla przedsiębiorstw. Mający za zadanie wdrożenie narzędzi rozliczalności (np. dokumentacji, oceny wpływu na prywatność itd), powinni być uznawani za „dyrygenta zgodności” oraz pośrednika pomiędzy wszystkimi odpowiednimi interesariuszami (np. organy nadzorcze, osoby, których dane dotyczą, partnerzy biznesowi).Grupa robocza popiera powołanie inspektora ochrony danych jako obowiązek przy zachowaniu obiektywnych kryteriów, takich jak rodzaj, ilość danych lub charakter działalności zainteresowanego podmiotu, co pomoże w pomiarze ryzyka”.*

- Urzędnik ds. ochrony danych osobowych (dyrektywa nr 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych)
- Administrator bezpieczeństwa informacji (art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych; art. 36b ust. 1 u.o.d.o. po nowelizacji dokonanej ustawą z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej
- Inspektor ochrony danych (rozdział IV, sekcja 4, art. 35 – 37 rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych)

Urzędnik odpowiedzialny za ochronę danych będący lub niebędący pracownikiem administratora danych musi mieć możliwość wykonywania swoich funkcji w sposób całkowicie niezależny (motyw 49 dyrektywy 95/46/we *in fine*),

Ale także motyw 54, art. 18 ust. 2, art. 20

„Niezależny” (SJP)

Niepodporządko-wany komuś, czemuś

Decydujący o sobie

Świadczący o braku podporządkowania komuś lub czemuś

Administrator bezpieczeństwa informacji (art. 36 ust. 3 w wersji ustawy obowiązującej do 31 grudnia 2014 r.)

„Administrator danych wyznacza administratora bezpieczeństwa informacji nadzorującego przestrzeganie zasad ochrony, o których mowa w ust. 1, chyba, że sam wykonuje te czynności.”

I stan obecny…(od 1 stycznia 2015 r.)

Administrator danych może powołać administratora bezpieczeństwa informacji (art. 36a ust. 1 u.o.d.o.).
Administrator bezpieczeństwa informacji podlega bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych (art. 36a ust. 7).
Administrator danych zapewnia środki i organizacyjną odrębność administratora bezpieczeństwa informacji niezbędne do niezależnego wykonywania przez niego zadań, o których mowa w ust. 2 (art. 36a ust. 8).
(aktualna wersja przepisu, po nowelizacji dokonanej ustawą z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej- art. 9).

Rozdział IV projektu rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych *Administrator i podmiot przetwarzający,* Sekcja 4 *Inspektor Ochrony Danych* (art. 35-37).

Obligatoryjne i fakultatywne przesłanki wyznaczenia Inspektora Ochrony Danych

„Wyobraźnia znaczy więcej, niż wiedza”
Albert Einstein

Obowiązek wyznaczenia inspektora ochrony danych w każdym przypadku, kiedy:

-przetwarzania dokonuje organ lub podmiot publiczny;

- przetwarzania dokonuje przedsiębiorstwo zatrudniające 250 osób lub więcej;
- główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania podmiotów danych.

Możliwości wyznaczenia jednego IOD (art. 35 ust. 1 projektu rozporządzenia):

-grupa przedsiębiorstw powyżej 250 pracowników,
-podmiot publiczny i jego jednostki organizacyjne,
-przypadki inne, niż wymienione w ust. 1.

Według danych dostępnych na stronie www.bip.stat.gov.pl na dzień 30 września 2015 r. było na terenie Polski:

- 4 180 675 przedsiębiorstw zatrudniających do 250 osób
- 4 445 przedsiębiorstw zatrudniających powyżej 250 osób

Inspektor Ochrony Danych to osoba:

- o odpowiednich kwalifikacjach zawodowych,
- posiadająca specjalistyczną wiedzę z zakresu prawa ochrony danych,
- praktykę,
- o zdolnościach do wykonywania zadań wskazanych w art. 37.

„Niezbędny poziom wiedzy specjalistycznej ustala się w szczególności zgodnie z prowadzonym przetwarzaniem danych oraz ochroną wymaganą dla danych osobowych przetwarzanych przez administratora lub podmiot przetwarzający.”

- Inne obowiązki zawodowe inspektora ochrony danych muszą być zgodne z zadaniami i obowiązkami tej osoby jako inspektora ochrony danych i nie mogą prowadzić do konfliktu interesu,
- kadencyjność IOD (co najmniej 2 lata; możliwość powtarzalności kadencji; określone warunki odwołania)
- podstawa współpracy – zatrudnienie lub umowa o świadczenie usług
- niezależność w wykonywaniu zadań:

„Administrator i podmiot przetwarzający dopilnowują, by inspektor ochrony danych wykonywał swoje obowiązki i zadania niezależnie i nie otrzymywał żadnych poleceń dotyczących pełnienia swojej funkcji. Inspektor ochrony danych podlega bezpośrednio kierownictwu administratora lub podmiotu przetwarzającego" (art. 36 ust. 2 projektu rozporządzenia).

- jawność informacji o IDO (imię, nazwisko, dane kontaktowe),
- zapewnienie IDO personelu, pomieszczeń, sprzętu i zasobów niezbędnych do wykonywania obowiązków i zadań wskazanych w art. 37

e-GIODO

Wyniki wyszukiwania w rejestrze ABI

wyświetlane 1-10 / 10177

Wyświetlanie wyników: 10 na stronie

Lp	Administrator	Kod	Miejscowość	Imię i nazwisko ABI
1	Gmina Miasta Zgierz	95-100	Zgierz	M. Koralewski
2	Sąd Rejonowy Katowice-Wschód	40-040	Katowice	D. Badocha
3	Pocztowe Towarzystwo Ubezpieczeń na Życie S.A.	02-672	Warszawa	J. Ziemba
4	Zespoł Szkół nr 2 w Dąbrowie Górniczej	41-303	Dąbrowa Górnicza	M. Mucha
5	Agencja Nieruchomości Rolnych	00-189	Warszawa	A. Jamrożek
6	Miejskie Przedsiębiorstwo Komunikacyjne S.A. w Krakowie	31-060	Kraków	M. Wawak
7	III Szpital Miejski im. dr Karola Jonschera w Łodzi	93-113	Łódź	E. Ślebocka
8	Specjalny Ośrodek Szkolno Wychowawczy dla Dzieci Słabo Widz	41-303	Dąbrowa Górnicza	S. Przywara
9	Powiat Zgierz	95-100	Zgierz	M. Koralewski
10	Gmina Ciężkowice	33-190	Ciężkowice	S. Jaremko

Strona: **1**, 2, 3, 4, ..., 1016, 1017, 1018

Inspektor Ochrony Danych - zadania

- informowanie administratora lub podmiotu przetwarzającego o ich obowiązkach wynikających z niniejszego rozporządzenia oraz dokumentowanie tej działalności i uzyskiwanych odpowiedzi;

- monitorowanie wykonania i stosowania polityk administratora lub podmiotu przetwarzającego w zakresie ochrony danych osobowych, w tym przydział obowiązków, szkolenie personelu zaangażowanego w operacje przetwarzania oraz powiązane kontrole;

- monitorowanie wykonania i stosowania niniejszego rozporządzenia, w szczególności jeśli chodzi o wymogi dotyczące uwzględnienia ochrony danych już w fazie projektowania, ochrony danych jako opcji domyślnej i bezpieczeństwa danych oraz informowania podmiotów danych, a także wniosków w ramach wykonywania praw przysługujących im na mocy niniejszego rozporządzenia.

- zapewnienie prowadzenia dokumentacji, o której mowa w art. 28;

Inspektor Ochrony Danych- zadania cd.

- monitorowanie dokumentacji, zgłoszeń i zawiadomień dotyczących naruszeń ochrony danych osobowych na mocy art. 31 i 32;

- monitorowanie przeprowadzenia oceny skutków w zakresie ochrony danych przez administratora lub podmiot przetwarzający oraz wniosków o uprzednie zezwolenie lub uprzednią konsultację, jeśli są one wymagane na mocy art. 33 i art. 34;

-monitorowanie odpowiedzi na wnioski organów nadzorczych oraz, w ramach kompetencji inspektora ochrony danych, współpraca z organem nadzorczym na wniosek tego organu lub z inicjatywy inspektora ochrony danych;

-pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem oraz zasięganie opinii organu nadzorczego, w odpowiednich przypadkach, z inicjatywy inspektora ochrony danych.

(art. 37 ust. 1 projektu rozporządzenia)

Plusy i minusy powołania IOD

„ZA”

- ranga ochrony danych (motywacja dla pracowników; sygnał dla podmiotów danych oraz kontrahentów, a także dla GIODO!)

„PRZECIW”

- dodatkowe koszty;
- konieczność zmian struktury organizacyjnej

INNE?

Sankcje administracyjne – art. 79 rozporządzenia.

Udzielenie ostrzeżenia na piśmie w przypadku pierwszego nieumyślnego naruszenia :
- przez osobę fizyczną / cele niekomercyjne
- przedsiębiorstwo do 250 pracowników/przetwarzanie danych jako działalność poboczna (ust. 3).

Sankcje do 1 miliona Euro/do 2% rocznego światowego obrotu przedsiębiorstwa - na każdy podmiot który „umyślnie lub lekkomyślnie” nie wskazuje inspektora ochrony danych lub nie zapewnia mu warunków umożliwiających wykonanie zadań na mocy art. 35, 36 i 37 (ust. 6j).

- „Oficer ochrony danych nie jest i nie będzie „agentem” GIODO, lecz swego rodzaju łącznikiem współpracującym z nim na bieżąco, przy zachowaniu jego pełnej niezależności. GIODO będzie przeprowadzał inspekcje dwiema drogami - poprzez sprawdzenia przez ABI-ch oraz poprzez kontrole jednostek, w których taki urzędnik nie został wyznaczony lub nie działa. Może to bowiem stanowić domniemanie, iż poziom ochrony danych osobowych w tych jednostkach jest niewystarczający.”

(Wykład Zastępcy GIODO)

-

Dyskusja...

Komentarze...

Pytania...

Refleksje...