CHRONPESEL.PL

URZĄD OCHRONY DANYCH OSOBOWYCH

KRAJOWY REJESTR DŁUGÓW www.krd.pl

„Zadania administratorów i inspektorów ochrony danych w kontekście bezpiecznego przetwarzania danych osobowych”

Raport z badania

Wrzesień 2022 r.

Spis treści

Jan Nowak
Prezes Urzędu Ochrony Danych Osobowych

Szanowni Państwo,

oddajemy w Wasze ręce trzecią część publikacji „Zadania administratorów i inspektorów ochrony danych w kontekście bezpiecznego przetwarzania danych osobowych" powstałą po przeprowadzeniu badania „Ochrona danych osobowych w 2022 r." pod patronatem Urzędu Ochrony Danych Osobowych.
Na podstawie informacji zgromadzonych w poprzednich dwóch częściach raportów już wiemy jak społeczeństwo rozumie ochronę danych osobowych, definiuje zasady ochrony danych osobowych czy potrafi przewidzieć konsekwencje swojego zachowania w przypadku nadmiernego udostępniania danych osobowych.

Niniejsza publikacja nawiązuje natomiast do jakże ważnej roli administratorów oraz inspektorów ochrony danych, jaką jest budowanie świadomości i kształtowanie odpowiednich postaw Polaków. Wskazuje również jakie są oczekiwania społeczeństwa względem tych podmiotów. Otóż ponad 60 proc. ankietowanych oczekuje od administratorów rzetelnej informacji, którą należy spełnić nie tylko w ramach tzw. obowiązku informacyjnego, ale przede wszystkim w przypadku wystąpienia naruszenia ochrony danych osobowych. Ankietowani chcieliby uzyskać od administratorów informacji na temat skutków naruszenia oraz rekomendacji działań, które powinni podjąć.

Ostatnia część raportu prezentuje także spostrzeżenia badanych na temat przepisów o ochronie danych osobowych w miejscu pracy. W tym zakresie uzyskane odpowiedzi nie napawają optymizmem. Prawie 1/3 osób pracujących zawodowo nie zna zasad ochrony danych osobowych obowiązujących w miejscu pracy. Ponadto blisko 2/3 ankietowanych zapewnia, że szkolenia na temat bezpieczeństwa danych osobowych nie są przeprowadzane regularnie.

Wszystkie te dane statystyczne świadczą o tym, że musimy jeszcze większą uwagę przykładać do edukacji całego społeczeństwa, a zwłaszcza pracowników, inspektorów ochrony danych oraz administratorów. Postawa każdego z nas ma wpływ na budowanie bezpiecznego i kompletnego systemu ochrony danych osobowych.

Zapraszam Państwa do lektury.

Adam Łącki
Prezes Zarządu Krajowego Rejestru Długów Biura Informacji Gospodarczej SA

Szanowni Państwo,

chciałbym serdecznie zaprosić do lektury trzeciej odsłony raportu na podstawie badania „Ochrona danych osobowych w Polsce w 2022 r.", który przygotowaliśmy wspólnie z ekspertami serwisu ChronPESEL.pl pod patronatem Urzędu Ochrony Danych Osobowych. Poprzednie publikacje dotyczyły tego, jaki jest nasz jako społeczeństwa stan wiedzy na temat bezpieczeństwa danych, czy wiemy, jak uniknąć aktualnych zagrożeń oraz jak radzimy sobie w starciu z oszustami wyłudzającymi dane osobowe.

Najnowszy raport poświęciliśmy roli, jaką w procesie budowania świadomości i bezpieczeństwa odgrywają administratorzy i inspektorzy danych osobowych. Jak wynika bowiem z przeprowadzonego badania, blisko 70 proc. Polaków nie wie, kto jest odpowiedzialny za przetwarzanie danych, zwłaszcza w sytuacjach kryzysowych, takich jak wyciek wrażliwych informacji. Co trzeci z nas uważa z kolei, że z konsekwencjami takich zdarzeń powinien radzić sobie sam poszkodowany.

Z tego wynika, że w zakresie edukacji musimy jeszcze wykonać bardzo dużą pracę. Jedną z ważniejszych przestrzeni takich działań powinno być miejsce pracy. Dlatego w raporcie zwracamy uwagę na rolę, jaką w tym procesie mają do odegrania administratorzy i inspektorzy danych osobowych. Publikacja zawiera szereg komentarzy ekspertów, którzy przybliżają te zagadnienia i udzielają konkretnych wskazówek, których stosowanie pomoże w zwiększeniu świadomości społeczeństwa.

Wierzę, że najnowszy raport będzie kolejnym krokiem na drodze do większego rozumienia naszych zadań i obowiązków, które budują ogólne bezpieczeństwo danych osobowych.

Zapraszam do lektury.

O badaniu

Badanie na zlecenie serwisu ChronPESEL.pl i Krajowego Rejestru Długów pod patronatem Urzędu Ochrony Danych Osobowych zostało przeprowadzone w I połowie 2022 roku metodą CAWI na reprezentatywnej grupie 1010 respondentów przez IMAS International.

Najważniejsze wnioski

70%

Blisko 70 proc. Polaków (68,8 proc.) nie wie, kto powinien się zająć neutralizacją skutków wycieku danych osobowych.

34,9%

Co trzeci badany (34,9 proc.) uważa, że z negatywnymi skutkami wycieku danych powinna sobie radzić osoba poszkodowana.

Ankietowani wskazują, że w przypadku wycieku danych, w pierwszej kolejności sprawą powinny się zająć organy ścigania (69,2 proc.), administrator, u którego doszło do naruszenia ochrony danych osobowych (60 proc.) oraz Urząd Ochrony Danych Osobowych (56,2 proc.).

51%

Tylko niewiele ponad połowa pracujących (51 proc.) wie, w jaki sposób pracodawca zabezpiecza ich dane osobowe, a trochę ponad 60 proc. wiedziałoby, komu należy zgłosić incydent związany z bezpieczeństwem danych.

Wyciek danych osobowych – obowiązki administratora

Rolę administratora definiuje art. 4 pkt 7 ogólnego rozporządzenia o ochronie danych (RODO), zgodnie z którym jest nim **„osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych”.**

Dla ustalenia, czy dany podmiot można uznać za administratora istotna będzie jego samodzielność w podejmowaniu decyzji o celach i sposobach przetwarzania danych.

Ogólne rozporządzenie o ochronie danych osobowych (RODO) to unijny akt prawny, który obowiązuje w sposób bezpośredni we wszystkich państwa Unii Europejskiej. Rozporządzenie określa prawa każdego z nas i obowiązki administratorów, czyli podmiotów, które decydują o celach i sposobach przetwarzania danych.

Przepisy RODO zapewniają każdemu z nas większą kontrolę nad naszymi danymi osobowymi, m.in. rozszerzając zakres obowiązków informacyjnych i zobowiązując administratorów, by komunikowali się z nami w zwięzły, łatwo dostępny i zrozumiały sposób. Na mocy RODO zyskaliśmy łatwiejszy dostęp do własnych danych oraz prawo do przenoszenia danych osobowych między usługodawcami. Mamy też prawo, by wszystkie sprawy dotyczące ochrony naszych danych kierować do krajowego organu ochrony danych, nawet gdy są one przetwarzane w innym państwie.

RODO dotyczy niemalże wszystkich, bo odnosi się do podmiotów, które przetwarzają dane osobowe w związku z działalnością zarobkową, zawodową, realizacją zadań publicznych bądź celów statutowych. Jego przepisy muszą więc stosować m.in. wszystkie urzędy, placówki oświaty, służby zdrowia, przedsiębiorcy (także ci najmniejsi, prowadzący np. małe zakłady fryzjerskie czy kosmetyczne), a także e-usługodawcy.

Unijne przepisy muszą być stosowane również przez przedsiębiorstwa działające poza UE, które oferują towary lub usługi obywatelom lub mieszkańcom państw unijnych lub które monitorują ich zachowania online. Zatem jeśli np. portal internetowy prowadzi podmiot z USA, ale z jego usług korzystają obywatele lub mieszkańcy państw UE, to w swojej działalności musi on przestrzegać unijnych zasad związanych z przetwarzaniem danych osobowych użytkowników.

Administratorzy powinni uwzględnić tzw. zasadę przejrzystości, która jest stosowana na wszystkich etapach komunikowania się z osobą, której dane są przetwarzane. Przesądza ona, że wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem danych osobowych mają być zwięzłe, przejrzyste i zrozumiałe oraz sformułowane jasnym i prostym językiem. Mają też być łatwo dostępne.

Administratorzy, dopełniając tzw. obowiązku informacyjnego, muszą podać swoją nazwę, adres, cel i podstawę prawną przetwarzania danych osobowych. Administratorzy muszą informować również m.in. o okresie, przez który dane osobowe będą przetwarzane (retencja danych), o ewentualnym fakcie profilowania i jego konsekwencjach czy też o danych kontaktowych inspektora ochrony danych, jeśli został on wyznaczony.

Zasada przejrzystości sprzyja m.in. odpowiedzialnemu i uczciwemu podejściu do wykorzystywania danych osobowych. Wskazywała, że jest to odpowiedź na oczekiwania osób fizycznych, które chcą zrozumiałych zasad postępowania z ich danymi oraz poczucia kontroli nad nimi. Wspomniana zasada służy budowaniu trwałych, bo opartych na wzajemnym zaufaniu, relacji między administratorami a osobami, których dane dotyczą, ale także pozyskiwaniu lojalności i otwartości tych osób.

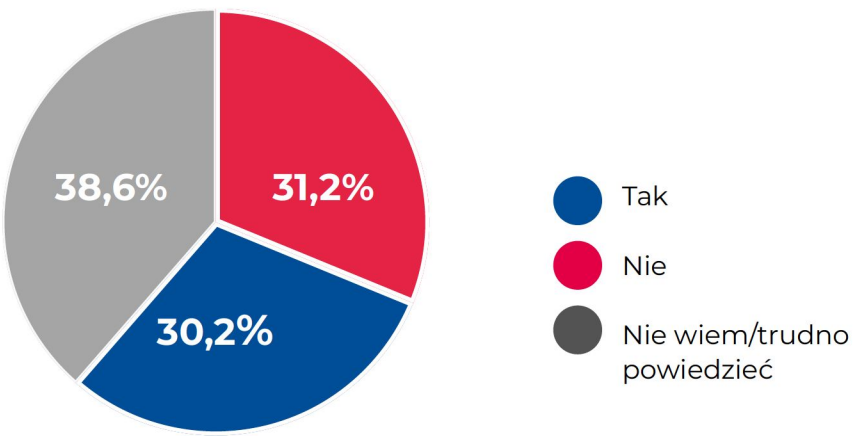
Ważne, aby administrator działał w taki sposób również w przypadku komunikatów o naruszeniu ochrony danych osobowych, który powinien dotrzeć do wszystkich osób fizycznych, na które dane naruszenie wywiera wpływ.

Tymczasem, jak wynika z przeprowadzonego badania, **zaledwie co trzeci Polak wie, kto w przypadku wycieku danych powinien się zająć neutralizacją jego negatywnych skutków.** Pozostali ankietowani deklarują, że nie wiedzą, na kim spoczywa ta odpowiedzialność.

Najczęściej twierdząco na to pytanie odpowiadały osoby w wieku 18–34 lata. Nadal było to jednak zaledwie między 35,5 a 37 proc. badanych. Najwięcej wątpliwości w tym zakresie zadeklarowali ankietowani między 35 a 44 r.ż. oraz seniorzy mający powyżej 65 lat. W tych grupach odsetek niewiedzących wyniósł około 75 proc.

Wykres 1

Czy wiesz, kto w momencie wycieku, powinien się zająć neutralizacją jego negatywnych skutków?



Ankietowani, którzy zadeklarowali, że wiedzą, kto powinien się zająć neutralizacją negatywnych skutków wycieku danych najczęściej wskazywali służby ścigania (np. policję czy prokuraturę) oraz firmę lub instytucję, która przetwarzała dane osobowe. Tak widziało to odpowiednio 69 proc. i 60 proc. badanych. Dalej na liście podmiotów, które powinny zmierzyć się ze skutkami wycieku danych ankietowani umieścili Urząd Ochrony Danych Osobowych (ponad 56 proc. wskazań) oraz inspektora ochrony danych z instytucji, w której doszło do naruszenia (ponad 44 proc.).

Za niepokojące należy jednak uznać prawie 35 proc. odpowiedzi, w których ankietowani uznali, że ze skutkami wycieku powinni sobie radzić sami poszkodowani. I to w wśród badanych, którzy wcześniej deklarowali, że potrafią wskazać odpowiedzialnego za te działania. Może to świadczyć o tym, że spora grupa osób może w takiej sytuacji poczuć się pozostawiona sama sobie.

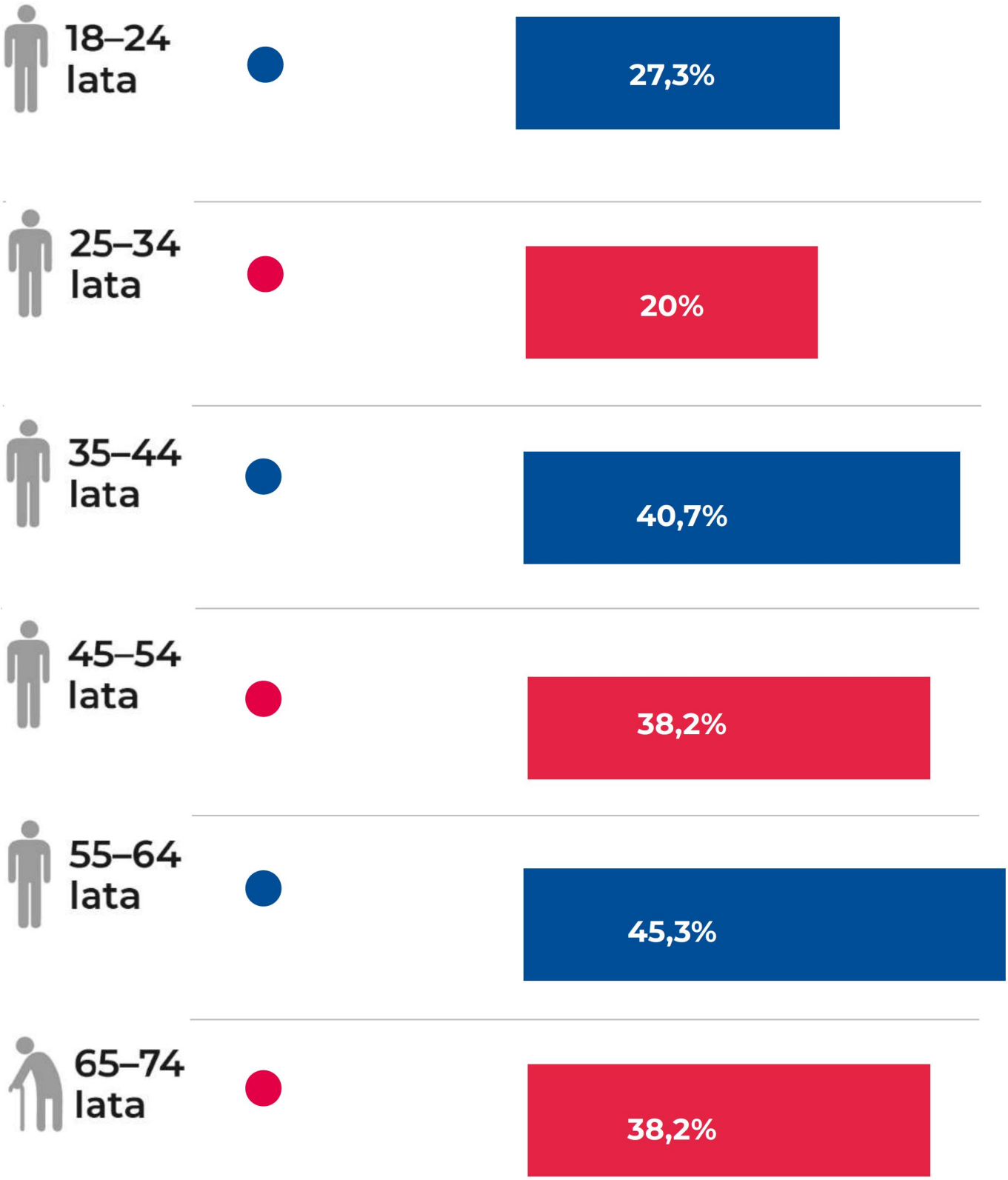
Wśród ankietowanych w wieku 55–64 lata ten odsetek wyniósł ponad 45 proc. Zdecydowanie rzadziej w ten sposób odpowiadali młodzi w wieku 18–24 lata (27,3 proc.) oraz 25–34 lata (20 proc.).

Wykres 2

Kto, w momencie wycieku danych, powinien zająć się neutralizacją jego negatywnych skutków?

Wykres 3

Kto uważa, że w przypadku wycieku danych neutralizacją jego negatywnych efektów powinien się zająć sam poszkodowany



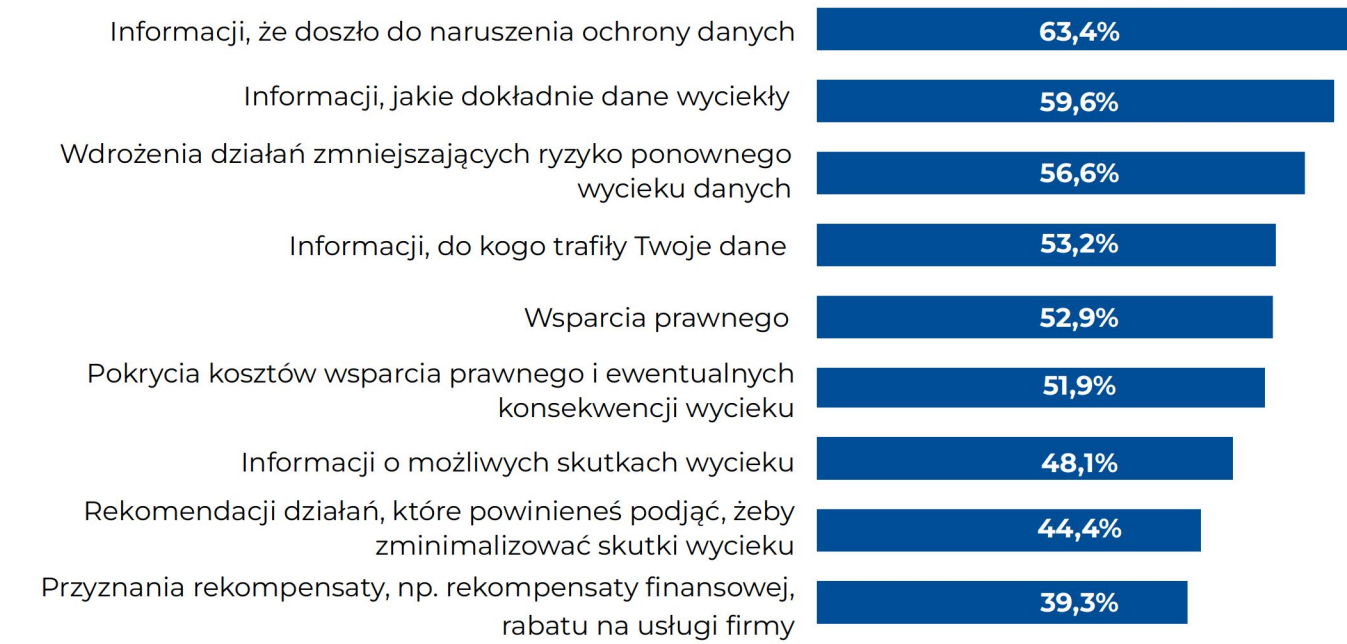
Z przeprowadzonego przez serwis ChronPESEL.pl i KRD pod patronatem UODO badania wynika, że poszkodowani od podmiotu odpowiedzialnego za wyciek ich danych osobowych oczekują przede wszystkim informacji – chcą jak najszybciej potwierdzić, że doszło do naruszenia ochrony danych osobowych (ponad 63 proc. ankietowanych) oraz jakie dane dokładnie ono objęło (prawie 60 proc.). Dodatkowo chętnie usłyszeliby lub przeczytali, co administrator zrobił, że uniknąć w przyszłości podobnych sytuacji (blisko 57 proc.), a także do kogo mogły trafić dane, które wyciekły (ponad 53 proc.).

Ponad połowa badanych oczekuje także wsparcia prawnego (53 proc.) lub pokrycia jego kosztów oraz wydatków, które będą związane z konsekwencjami naruszenia (52 proc.). Ankietowani chcieliby także dowiedzieć się od administratora, jakie mogą być skutki takiej sytuacji oraz rekomendacji działań, które powinni podjąć (48 proc.), żeby zminimalizować skutki wycieku (ponad 44 proc.).

Prawie 40 proc. badanych uważa, że odpowiedzialny za wyciek danych osobowych powinien udzielić poszkodowanym rekompensaty finansowej za poniesione straty lub rabatu na własne usługi.

Wykres 4

Jakiego rodzaju działań oczekujesz od podmiotu odpowiedzialnego za wyciek Twoich danych osobowych?



Wyciek danych osobowych – obowiązki administratora

Administrator wdraża środki techniczne i organizacyjne, zapewniające odpowiedni stopień bezpieczeństwa. Na podstawie art. 24 RODO administrator jest zobowiązany uwzględniać: charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, i odpowiednio do nich dobierać oraz wdrażać środki techniczne i organizacyjne tak, aby przetwarzanie odbywało się zgodnie z rozporządzeniem i móc to wykazać. Środki te powinny być w razie potrzeby poddawane przeglądom i uaktualniane. Ponadto zarówno przy określaniu ilości zbieranych danych osobowych, jak i zakresu ich przetwarzania, okresu przechowywania, dostępności oraz sposobów przetwarzania konieczne jest stosowanie mechanizmów takich jak zapewnienie ochrony danych osobowych na etapie projektowania oraz domyślnej ochrony danych („privacy by design" oraz „privacy by default"), zarówno przed przystąpieniem do przetwarzania danych, jak i w czasie prowadzonego przetwarzania (art. 25 RODO).

Administrator musi się liczyć także z odpowiedzialnością odszkodowawczą, o której mowa w art. 82 RODO. Zgodnie z tym przepisem, każda osoba, która poniosła szkodę majątkową lub niemajątkową spowodowaną naruszeniem przepisów RODO, będzie miała prawo dochodzić od administratora lub podmiotu przetwarzającego odszkodowania. Jeśli nie dojdą do porozumienia, wówczas sprawa trafi do sądu cywilnego.

Zdaniem eksperta

Jacek Młotkiewicz
dyrektor Departamentu Kontroli i Naruszeń, UODO

W każdej sytuacji administrator powinien pamiętać, że dane osobowe muszą być przez niego przetwarzane w sposób zapewniający bezpieczeństwo tych danych za pomocą odpowiednich środków technicznych lub organizacyjnych. Administrator, ustalając te środki, powinien uwzględnić charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, zagrożenia wynikające z przetwarzania, a także stan wiedzy technicznej oraz koszt wdrażania danego rozwiązania. Zastosowane przez administratora środki powinny być poddawane przeglądom i aktualizacji.
Zatem ustalenie odpowiednich środków technicznych i organizacyjnych jest procesem dwuetapowym. W pierwszej kolejności istotnym jest określenie poziomu ryzyka, jakie wiąże się z przetwarzaniem danych osobowych, a następnie administrator ustala, jakie środki techniczne i organizacyjne będą odpowiednie, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

Zdaniem eksperta

Bartłomiej Drozd
ekspert serwisu ChronPESEL/PL

Niestety z konsekwencjami wycieku danych w postaci np. zobowiązań finansowych zaciągniętych na nasze nazwisko, możemy się mierzyć na długo po zaistnieniu incydentu. Dlatego bardzo ważne jest, żeby jak najszybciej ustalić, jakie dokładnie dane wyciekły i kiedy. W takich sytuacjach czas reakcji ma bowiem ogromne znaczenie. Całą sprawę utrudnia również fakt, że bezpieczeństwo baz danych, nie zależy od nas, a od podmiotów, które nimi zarządzają. Dlatego istotne jest także to, żeby wiedzieć, do kogo się zgłosić i jakie działania należy podjąć. Przykładowo, jeśli wśród informacji, które wyciekły znalazły się także dane osobowe, np. numer PESEL, należy jak najszybciej sprawdzić, czy ktoś nie próbował ich już wykorzystać. Warto pomyśleć także nad uruchomieniem monitoringu aktywności kredytowej naszego numeru PESEL, dzięki temu dowiemy, jeśli w przyszłości ktoś będzie chciał wyłudzić na niego pożyczkę lub inne zobowiązanie finansowe.

Inspektor ochrony danych i jego rola

Jak wynika z przepisów RODO, na administratorach ciąży obowiązek starannego i przemyślanego wyboru osoby, którą wyznaczy do pełnienia roli inspektora ochrony danych (IOD) w swojej firmie bądź instytucji.

Kto może, a kto musi wyznaczyć IOD na podstawie RODO?

RODO w art. 37 ust 1 RODO przewiduje obowiązek wyznaczenia inspektora przez administratorów i podmiotów przetwarzających wówczas, gdy:

1. Przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości.

2. Główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą na dużą skalę.

3. Główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO oraz danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o których mowa w art. 10 RODO.

Zgodnie z art. 37 ust. 6 RODO inspektorem ochrony danych może zostać zarówno pracownik administratora lub podmiotu przetwarzającego, jak i osoba spoza grona pracowników ww. podmiotów (outsourcing).

Rozporządzenie precyzuje także zadania inspektora.

Jakie zadania ma IOD?

Do zadań inspektora ochrony danych zgodnie z art. art. 39 ust. 1 oraz 38 ust. 4 RODO należą:

1. Informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie.

2. Monitorowanie przestrzegania RODO, innych przepisów UE lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty.

3. Udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO.

4. Współpraca z Prezesem Urzędu Ochrony Danych Osobowych.

5. Pełnienie funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

Rola inspektora ochrony danych jest kluczowa dla zbudowania skutecznego systemu ochrony danych osobowych danego podmiotu. Zadaniem IOD jest nie tylko wspieranie administratora w takim zorganizowaniu procesów przetwarzania danych osobowych, aby dane te były należycie chronione, ale także stałe monitorowanie, czy dana organizacja działa zgodnie z prawem. Ponadto inspektor może podejmować działania zwiększające świadomość pracowników co do zasad ochrony danych osobowych. Jego zadaniem jest także udzielanie informacji osobom, których dane dotyczą. Taką rolę IOD pełni w odniesieniu do organu nadzorczego, z którym ma się kontaktować we wszystkich możliwych sprawach.

Zdaniem eksperta

Monika Krasińska
dyrektor Departamentu Orzecznictwa i Legislacji, UODO

Choć za przetwarzanie danych osobowych zgodnie z RODO odpowiedzialny jest administrator, czyli podmiot, który decyduje o celach i sposobach przetwarzania danych, to w realizacji związanych z tym zadań wspierać go może – a w niektórych przypadkach, jak np. w sektorze publicznym, wręcz musi – specjalista, jakim jest inspektor ochrony danych (IOD). IOD z jednej strony ma doradzać administratorowi, jak prawidłowo zorganizować i realizować procesy przetwarzania danych osobowych, z drugiej zaś monitorować i weryfikować, czy wynikające z RODO obowiązki są prawidłowo wykonywane. Jego rolą jest także podejmowanie działań zwiększających świadomość w zakresie ochrony danych osobowych, w tym szkolenie personelu uczestniczącego w operacjach przetwarzania.

Ważnym zadaniem IOD jest też pełnienie roli punktu kontaktowego, czyli pośrednika między administratorem lub podmiotem przetwarzającym a osobami, których dane dotyczą, oraz między administratorem lub podmiotem przetwarzającym a organem nadzorczym.

Co istotne, IOD nie może być osobą, która wyręcza administratora w realizacji należących do niego zadań. Mogłoby to bowiem prowadzić do powstania konfliktu interesów, co stanowiłoby naruszenie przepisów RODO.

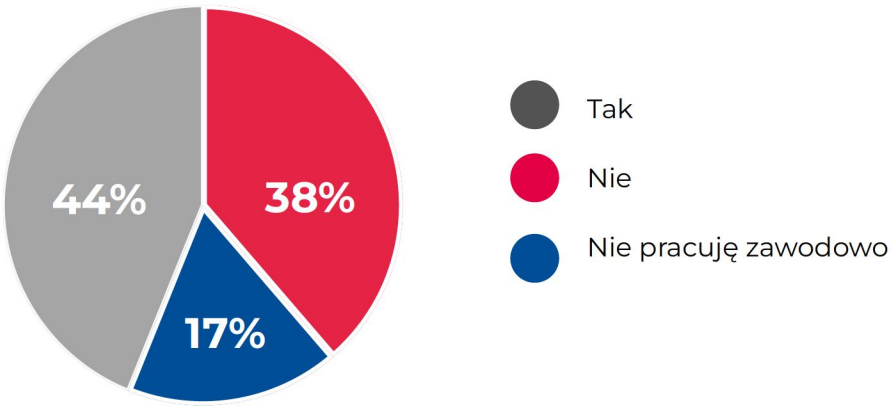
Warto też podkreślić, że IOD nie jest osobą, która jako jedyna w organizacji ma odpowiadać za właściwą ochronę danych osobowych. Powinni dbać o nią wszyscy, którzy są zaangażowani w procesy przetwarzania danych, zwłaszcza zaś kierownictwo.

Ochrona danych osobowych w miejscu pracy

Przeprowadzone badanie dotyczyło także znajomości procedur dotyczących ochrony danych osobowych w miejscu pracy. Zapytani o to pracujący (blisko 39 proc. wszystkich ankietowanych) w większości (prawie 69 proc.) odpowiedzieli twierdząco. Na co należy zwrócić uwagę? Prawie 1/3 pracujących zawodowo osób nie zna zasad ochrony danych osobowych obowiązujących w ich miejscach pracy.

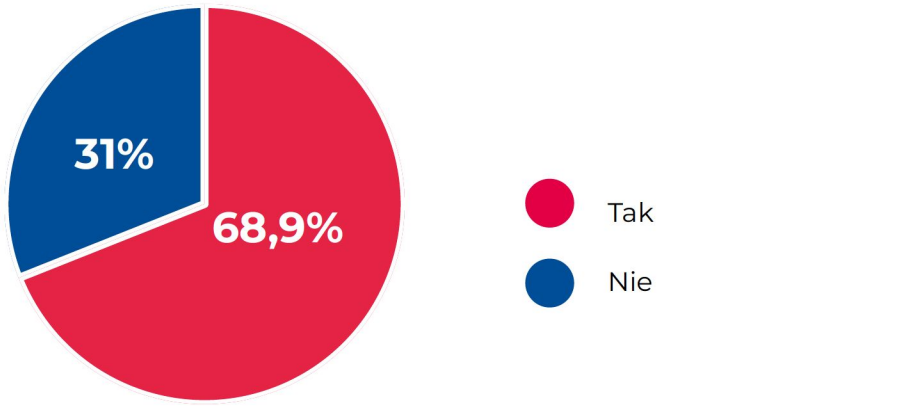
Wykres 5

Czy znasz zasady ochrony danych osobowych obowiązujące w Twoim miejscu pracy?



Wykres 6

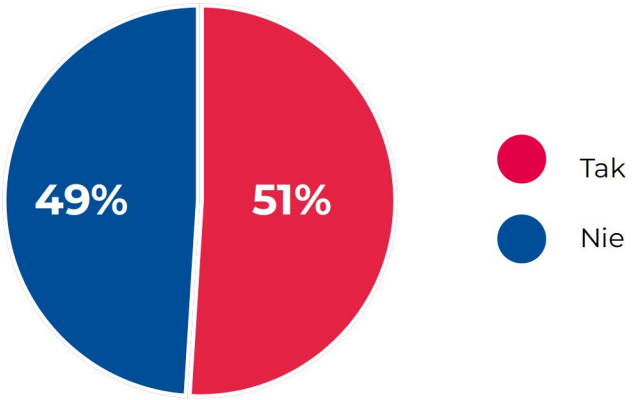
Osoby pracujące zawodowo
Czy znasz zasady ochrony danych osobowych obowiązujące w Twoim miejscu pracy?



Podczas badania zapytano pracowników o to, czy wiedzą, w jaki sposób pracodawca zabezpiecza ich dane osobowe. Twierdząco odpowiedziała bowiem zaledwie niewiele ponad połowa z nich (51 proc.). Najwyższy poziom świadomości na ten temat ponownie prezentują ludzie młodzi, w wieku 18–24 lata – 67,7 proc. Następnie deklarowany stan wiedzy obniża się wraz ze wzrostem wieku ankietowanych. Jak wynika z przeprowadzonego badania, powyżej 35 r.ż. więcej jest osób, które nie wie, jak pracodawca chroni ich dane osobowe.

Wykres 7

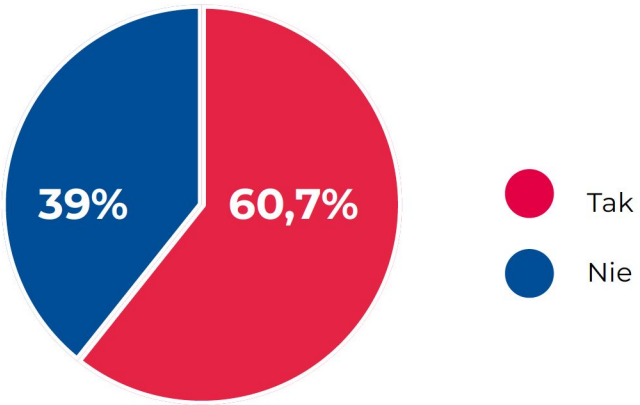
Czy wiesz, w jaki sposób pracodawca zabezpiecza Twoje dane osobowe?



Więcej ankietowanych pracowników wie z kolei, do kogo u pracodawcy powinno się zgłosić incydent związany z bezpieczeństwem danych osobowych, np. wyciek danych. Na to pytanie twierdząco odpowiedziało ponad 60 proc. ankietowanych. Najlepiej przygotowane do takich sytuacji są osoby w wieku 18–34 lata – od 64,5 proc. do 66,7 proc. Najgorzej badani w grupie 35–44 lata – niewiele ponad połowa (ponad 52 proc.) wie, komu w pracy powinna zgłosić takie incydenty.

Wykres 8

Czy wiesz, do kogo w firmie powinieneś się zgłosić w przypadku wycieku danych/incydentu związanego z bezpieczeństwem danych osobowych?



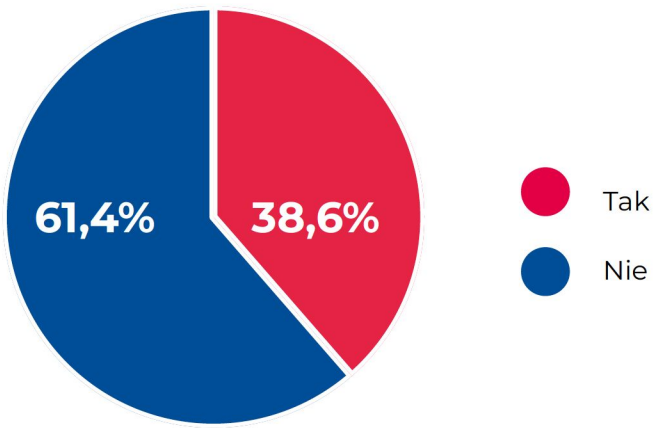
Taki stan deklarowanej wiedzy nie musi wynikać wyłącznie z zaniechań po stronie pracodawcy. Trudno jednak zachować optymizm, jeśli blisko 2/3 ankietowanych zapewnia, że szkolenia na temat bezpieczeństwa danych osobowych nie są organizowane regularnie. Za wyjątkiem najmłodszej grupy respondentów, podobny odsetek występuje w każdej grupie wiekowej, dlatego nie można założyć, że poniższe odpowiedzi wynikają jedynie z ignorancji pracowników.

Przykładami naruszeń występujących na skutek niewłaściwego postępowania pracownika są: wysyłanie poczty elektronicznej do wielu adresatów, udostępnienie adresatowi korespondencji danych innej osoby poprzez nieprawidłowe zaadresowanie bądź spakowanie przesyłki (zarówno tej tradycyjnej, jak i wysyłanej drogą elektroniczną), pomyłka w adresie e-mail adresata z powodu jego błędnego wpisania w momencie wysyłki lub wprowadzenia niewłaściwych danych do sytemu informatycznego (np. wprowadzenie na koncie klienta adresu e-mail/adresu korespondencyjnego innego klienta), czy udostępnienie osobie nieuprawnionej danych w formie papierowej lub elektronicznej. Do naruszeń może również dojść w skutek: omyłkowo zaksięgowanych przelewów, wydawania dokumentów (np. formularzy) zawierających dane osobowe innych osób czy braku uprawnień osób zgłaszających się z wnioskiem o udostępnienie dokumentów czy danych.

W działalności administratorów zdarzyć się może również zniszczenie, kradzież dokumentacji bądź niezabezpieczonych (niezaszyfrowanych) urządzeń informatycznych (smartfonów, komputerów przenośnych, nośników danych) zawierających dane osobowe. Może również dojść do zagubienia dokumentów zawierających dane osobowe (np. klienta/-ów). Dlatego tak ważne jest ustalenie zasad ochrony danych osobowych, polityk bezpieczeństwa danych osobowych w każdej organizacji oraz odpowiednie szkolenia personelu.

Wykres 9

Czy Twój pracodawca zapewnia regularne szkolenia z wiedzy na temat bezpieczeństwa danych osobowych, informuje o zmianach w przepisach itd.?



Zdaniem eksperta

Jacek Młotkiewicz
dyrektor Departamentu Kontroli i Naruszeń, UODO

Analiza naruszeń ochrony danych osobowych zgłaszanych do UODO wskazuje, że administratorzy podejmują różne działania, które mają eliminować w przyszłości występowanie zdarzeń naruszających ochronę danych osobowych. Do popularnych rozwiązań należy przeprowadzanie dodatkowych, właściwie ukierunkowanych tematycznie i osobowo szkoleń personelu, obejmujących analizę zaistniałych naruszeń/zdarzeń niepożądanych. W ocenie UODO przeprowadzanie szkoleń pracowników w zakresie ochrony danych osobowych jest konieczne i potrzebne.

Jednak szkolenia nie można uznać za wdrożenie wystarczających środków organizacyjnych, nie powinny one zastępować także rozwiązań o charakterze technicznym. Dla przykładu warto również wprowadzić:

- przeglądy i udoskonalanie, w tym upraszczanie przekazów wynikających z procedur,
- audyty bezpieczeństwa i stosowanie wynikających z nich wniosków,
- procedury udostępniania danych z uwzględnieniem przepisów szczególnych oraz opisem pojawiających się w tym zakresie błędów,
- systematyczną weryfikację ważności i zakresu uprawnień dostępu do danych osobowych,
- weryfikację umów zawartych z podmiotami zewnętrznymi, np. operatorem pocztowym, z uwzględnieniem zidentyfikowanych nieprawidłowości.

Zdaniem eksperta

Małgorzata Dulińska-Majkowska
Inspektor ochrony danych w Kaczmarski Group Sp. j.

Mając na uwadze, że zdarzają się naruszenia ochrony danych osobowych występujące na skutek. działania pracowników, ich edukacja w zakresie ochrony danych osobowych jest bardzo ważna. Oprócz standardowych szkoleń wstępnych warto zadbać o dodatkowe elementy, np. regularny newsletter do wszystkich pracowników dotyczący tego tematu oraz wyjaśniający przepisy prawa i ich zmiany. Warto powiązać to także z zagadnieniami dotyczącymi cyberbezpieczeństwa. Jest to temat bardzo aktualny, także ze względu na coraz to nowsze pomysły przestępców na oszustwa. Dobrze, żeby pracownicy zdawali sobie sprawę z bieżących zagrożeń, ponieważ ma to także wpływ na ich zachowanie w czasie pracy. Bezwzględnie także każdy z nich powinien wiedzieć, kto w firmie pełni funkcję inspektora ochrony danych i do kogo powinni zgłaszać wszystkie incydenty lub zagrożenia, które zauważyli. Ze względu na naturalną rotację, takie działania edukacyjne powinny mieć charakter ciągły.

Autorzy raportu

ChronPESEL.pl – misją serwisu ChronPESEL.pl jest zwiększenie poziomu bezpieczeństwa i ograniczenie ryzyka wystąpienia negatywnych konsekwencji utraty danych osobowych oraz kradzieży tożsamości. Korzystając z najnowszych rozwiązań technologicznych, ChronPESEL.pl monitoruje w czasie rzeczywistym potencjalne próby wyłudzeń, dzięki czemu można im zapobiegać z dużo większą skutecznością. Prowadzi również aktywne działania edukacyjne mające na celu zwiększenie świadomości aktualnych zagrożeń oraz poznanie zasad bezpieczeństwa.

Krajowy Rejestr Długów Biuro Informacji Gospodarczej SA – najstarsze i największe biuro informacji gospodarczej w Polsce działające od 4 sierpnia 2003 roku pod nadzorem Ministerstwa Rozwoju i Technologii. Lider na rynku informacji gospodarczej, administrujący bazą danych o 2,7 mln dłużników. Z usług KRD korzysta blisko 930 tysięcy przedsiębiorców i konsumentów, którzy rocznie pobierają 34 miliony raportów gospodarczych. KRD BIG SA wchodzi w skład Kaczmarski Group, do którego należą również takie firmy i marki, jak: firma windykacyjna Kaczmarski Inkasso, Rzetelna Firma, Kancelaria Prawna VIA LEX, firma faktoringowa NFG, ChronPESEL.pl oraz Easy Check.

Prezes Urzędu Ochrony Danych Osobowych jest organem nadzorczym powołanym do przestrzegania przepisów RODO. Wykonuje swoje zadania przy pomocy Urzędu Ochrony Danych Osobowych. Niezależność Prezesa UODO i kierowanego przez niego Urzędu jest gwarantowana przez ogólne rozporządzenie o ochronie danych osobowych.

Zadania Prezesa UODO określa RODO, do których należy m.in.: monitorowanie i egzekwowanie stosowania rozporządzenia ogólnego o ochronie danych; upowszechnianie w społeczeństwie wiedzy o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem danych; upowszechnianie wśród administratorów i podmiotów przetwarzających wiedzy o obowiązkach spoczywających na nich na mocy RODO; rozpatrywanie skarg wniesionych przez osoby, których dane dotyczą ; analiza naruszeń u administratorów; prowadzenie postępowań administracyjnych w związku z ochroną danych osobowych. Do uprawnień organu nadzorczego należy m.in. nakładanie kar pieniężnych (art. 58 RODO). Jednak karanie administratorów danych nie jest celem samym w sobie. Dlatego UODO w pierwszej kolejności – jeśli w ogóle jest taka potrzeba – korzysta z takich uprawnień, jak upomnienia, ostrzeżenia czy wezwania do przywrócenia stanu, w którym przetwarzanie danych odbywa się zgodnie z prawem.

Prezes Urzędu jest również członkiem Europejskiej Rady Ochrony Danych Osobowych.

CHRONPESEL.PL

URZĄD OCHRONY DANYCH OSOBOWYCH

KRAJOWY REJESTR DŁUGÓW www.krd.pl

Kontakt dla mediów

ChronPESEL.pl Jan Garnecki | media@chronpesel.pl

Krajowy Rejestr Długów BIG SA Andrzej Kulik | media@krd.pl

Urząd Ochrony Danych Osobowych Adam Sanocki | rzecznikprasowy@uodo.gov.pl