ZFODO

Incydenty ochrony danych osobowych

Raport Związku Firm Ochrony Danych Osobowych

00 O raporcie

- Badaniem objęliśmy **277 organizacji** obsługiwanych przez firmy zrzeszone w ramach ZFODO w okresie **maj 2018–maj 2019**.
- Na obsługiwane organizacje składa się zarówno sektor publiczny, jak i sektor prywatny.
- Obsługiwane organizacje współpracowały z firmami zrzeszonymi w ramach ZFODO w zakresie outsourcingu IOD lub innej stałej współpracy w zakresie ochrony danych osobowych.

01

Prawdopodobieństwo wystąpienia incydentu

127
odnotowanych incydentów

277
organizacji

0,46
średnia liczba incydentów przypadających na organizację

- **Raportem objęliśmy 277 organizacji, obsługiwanych przez 8 różnych firm zrzeszonych w ramach ZFODO. Łącznie w okresie od 25 maja 2018 do 25 maja 2019, w ww. liczbie organizacji, odnotowano oficjalnie 127 incydentów.**

Daje to średnią 0,46 incydentu rocznie na każdą organizację. Badanie opieramy na incydentach, które zostały zgłoszone firmom zrzeszonym w ZFODO przez obsługiwane przez nich organizacje. Liczba incydentów, które wystąpiły w rzeczywistości może być wyższa.

ZFODO mówi...

Przemysław Zegarek

PREZES ZARZĄDU LEX ARTIST SP. Z O.O.

Statystyka pokazuje, że powinniśmy być gotowi (w przybliżeniu) na jeden incydent danych osobowych w przeciągu dwóch lat. To niewiele. Powyższe liczby mogą być mylące z dwóch powodów:

1. Branże b2b, stosunkowo mało incydentogenne, zaniżają znacząco statystykę. Jeśli Twoja organizacja bezpośrednio obsługuje osoby fizyczne, prawdopodobieństwo incydentu będzie wyższe.

2. Poziom raportowania incydentów w organizacjach wciąż pozostawia wiele do życzenia. Wszyscy uczymy się skutecznie odróżniać sprawy błahe, nie wymagające raportowania, nie wyrządzające nikomu szkody, od tych naprawdę poważnych i generujących ryzyka.

Magdalena Chmielewska

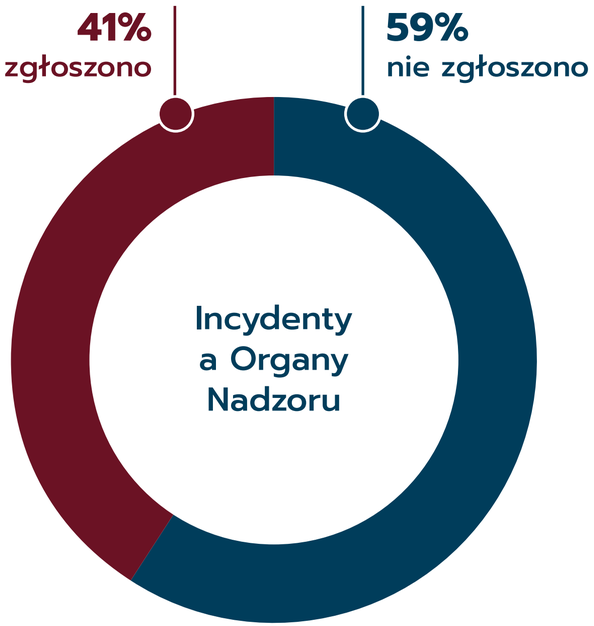
PREZES ZARZĄDU ODO MANAGEMENT GROUP SP. Z O.O.

Biorąc pod uwagę przedstawione dane można by sadzić, że prawdopodobieństwo incydentu na poziomie 0,46 % w przeliczeniu na organizację w skali roku nie jest wysokim czynnikiem, jednakże w sytuacji gdy zbadanych zostało 277 organizacji, a okres badania przypadał na pierwszy rok stosowania RODO, nie sposób oprzeć się wrażeniu, że to wysoki współczynnik – szczególnie, gdy zestawi się go z 89% procentowym wskaźnikiem osobowych przyczyn wystąpienia incydentów.

Zidentyfikowane 0,46% może być wynikiem niedostatecznej świadomości osób przetwarzających dane osobowe w klasyfikowaniu incydentów oraz zarządzaniu tymi zdarzeniami. Wg naszej opinii przez okres kolejnego roku wskaźnik incydentów będzie rósł w miarę wzrostu świadomości organizacji związanej z zagrożeniami płynącymi z przetwarzania danych. Dowodzi to, że organizacje nie były gotowe na stosowanie RODO w momencie jego wejścia w życie.

02

Incydenty zgłoszone Organowi Nadzoru



- **Blisko 60% incydentów, nie zostało zgłoszonych do regulatora. Zgodnie z art. 33 ust. 1 RODO, incydentu możemy nie zgłaszać regulatorowi, jeśli „jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych”.**

Dokonanie samodzielnej oceny małego lub dużego prawdopodobieństwa naruszenia praw lub wolności budzi w wielu sytuacjach trudności i obawy oceniających.

ZFODO mówi...

Agata Kłodzińska

EKSPERT DS. OCHRONY DANYCH ODO 24 SP. Z O.O.

Stosunek administratorów do zgłaszania naruszeń organowi nadzorczemu należy ocenić dwuznacznie: z jednej strony administratorzy mają obawy przed zgłoszeniem, które utożsamiają z potencjalnym zwróceniem na siebie uwagi organu, co może wpłynąć na niższy odsetek zgłoszeń, a z drugiej – mają świadomość konsekwencji, które grożą im za brak raportowania naruszeń.

Wydaje się jednak, że im dłużej stosowane jest RODO, tym mniej problemów sprawia ocena charakteru naruszenia – m.in. dzięki opracowywanym przez ekspertów metodom wyliczania prawdopodobieństwa naruszenia praw i wolności osób fizycznych, takim jak kalkulatory wagi naruszeń bazujące na zaleceniach ENISA, a także dzięki doświadczeniu administratorów zdobywanemu podczas obsługi kolejnych naruszeń.

Przemysław Zegarek

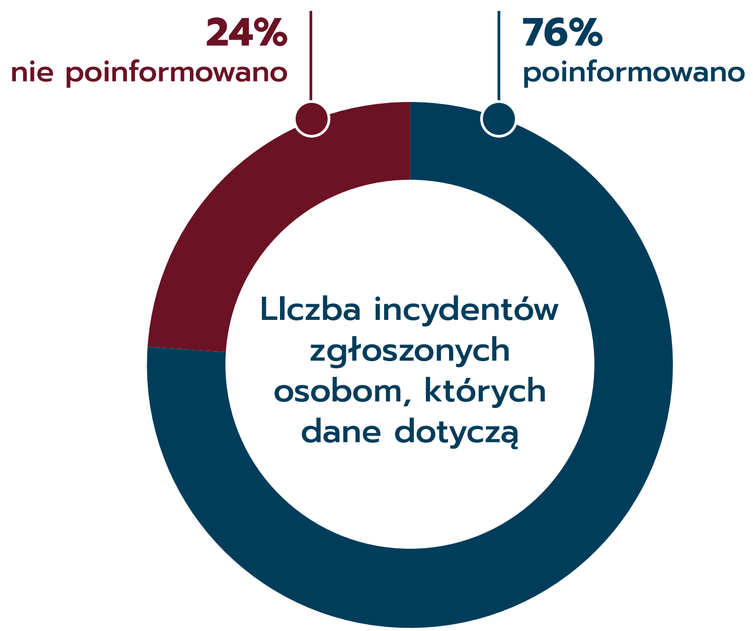
PREZES ZARZĄDU LEX ARTIST SP. Z O.O.

Ocena wagi i szkodliwości incydentu, za każdym razem musi zostać przygotowana indywidualnie. To przedstawiciel administratora danych podejmuje decyzję i bierze za nią odpowiedzialność. Tym co mi pomaga przy doradzaniu w podobnych sprawach, jest świadomość sposobu funkcjonowania regulatora i prawa w ogólności.

Jeśli przeprowadziliśmy rzetelną i obiektywną analizę trudnej i niejednoznacznej sytuacji nt. zgłaszać czy nie zgłaszać, to sam ten fakt jest bardzo ważny.

Nawet jeśli finalnie zdaniem regulatora okaże się, że incydent jednak powinien być zgłoszony, to sam fakt odnotowania naszej analizy w wewnętrznej dokumentacji – zadziała na naszą korzyść.

03 Incydenty zgłoszone osobom, których dane dotyczą



- **Niezależnie od zgłoszenia incydentu do regulatora, zgodnie z art. 34 RODO „jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych" to powinniśmy o nim poinformować także same osoby objęte naruszeniem.**

Podobnie jak w przypadku raportowania incydentów do regulatora, ocena wysokiego ryzyka naruszenia praw lub wolności, budzi trudności interpretacyjne.

W nieco ponad ¾ przypadków osoby decyzyjne, uznały, że incydenty mogły powodować wysokie ryzyko naruszenia praw lub wolności. Tym samym konieczne było poinformowanie osób, których dotyczyło naruszenie.

ZFODO mówi...

Michał Sztąberek

PREZES ZARZĄDU iSECURE SP. Z O.O.

Zawiadomienie poszkodowanego o naruszeniu to realny problem dla firm. RODO zawiera pewne wskazówki w tym zakresie, ale praktyka pokazuje, że łatwo jest popełnić błąd, którego konsekwencją będzie stresująca korespondencja z PUODO, w której organ domagać się będzie uszczegółowienia informacji wysłanej do zainteresowanego.

Istotny jest zwłaszcza opis możliwych konsekwencji naruszenia, np. gdy wyciekły: imię, nazwisko oraz PESEL, należy przykładowo wskazać, że możliwe jest sfałszowanie tożsamości poprzez uzyskanie przez osoby trzecie, na szkodę pokrzywdzonego, kredytów w instytucjach pozabankowych bądź wyłudzenia środków z ubezpieczenia.

Przemysław Zegarek

PREZES ZARZĄDU LEX ARTIST SP. Z O.O.

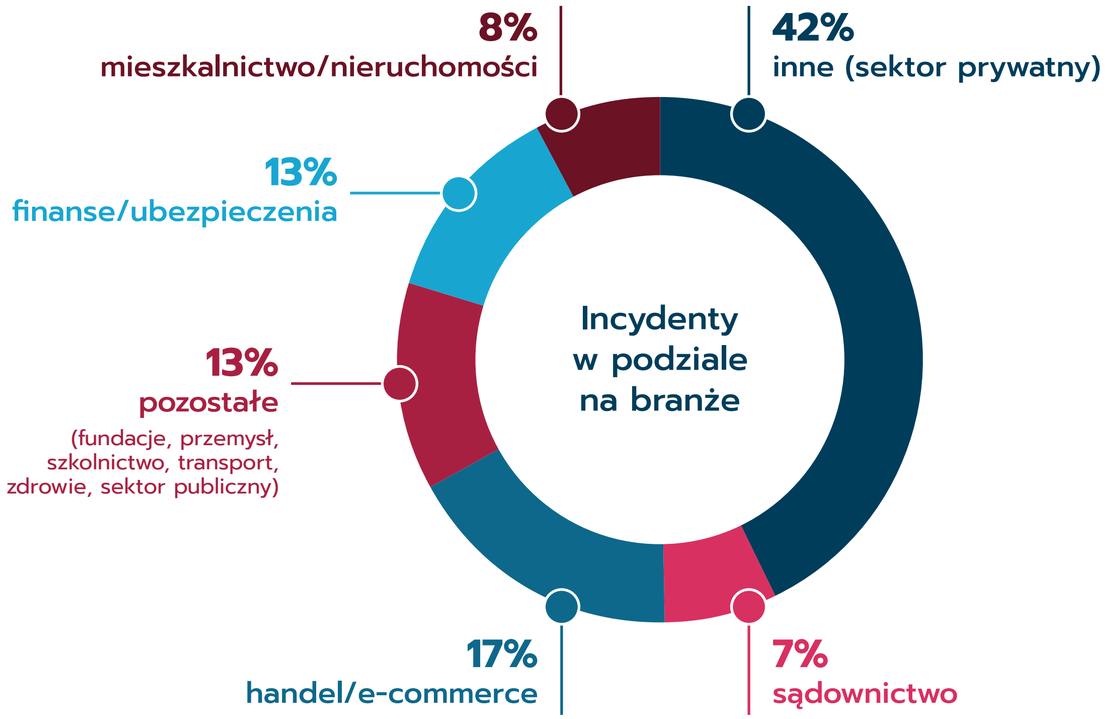
Wysokie ryzyko naruszenia praw lub wolności – to termin oceny, wymagający indywidualnej analizy w każdym możliwym przypadku.

Jeśli uznamy, że ryzyko naruszenia praw lub wolności jest duże, to musimy o naruszeniu poinformować również osoby, których ono dotyczyło. Mogą to być nasi klienci bądź pracownicy. Taka decyzja wymaga dużo odwagi ze strony administratora danych. Pojawić się mogła pokusa naginania przepisu do własnych potrzeb i negowania ryzyka.

Statystka tego nie potwierdza. W większości przypadków o incydencie informowano również osoby, których prywatności była zagrożona.

04

Branże najbardziej narażone na ryzyko naruszeń ochrony danych osobowych



- **Sektor prywatny wygenerował aż 80% wszystkich incydentów odnotowanych przez ZFODO. Nie można jednak wyciągnąć z tego zbyt daleko idących wniosków. Szczególnie silna obecność sektora prywatnego może świadczyć również o tym, że firmy zrzeszone w ZFODO obsługują w większości sektor prywatny.**

Warto zwrócić uwagę na to, że branże takie jak handel/e-commerce oraz finanse/ubezpieczenia wygenerowały łącznie aż 30% wszystkich incydentów.

ZFODO mówi...

Maria Lothamer

WICEPREZES ZARZĄDU iSECURE SP. Z O.O.

To prawda, że otrzymany tutaj wynik, nie do końca odzwierciedla rzeczywiste ryzyko naruszeń w branżach z sektora publicznego oraz prywatnego, w związku ze współpracą firm zrzeszonych w ZFODO głównie z sektorem prywatnym.

Tak naprawdę ryzyko naruszenia występuje w każdej organizacji i nie ma znaczenia sektor czy branża jaką reprezentuje. Znaczenie ma rodzaj gromadzonych przez te organizacje danych (w tym przypadku może pojawić się większe ryzyko kradzieży danych, np. informacji o stanie zdrowia, numerów kart kredytowych), sposoby przetwarzania danych oraz niewiedza wśród pracowników, a to właśnie błąd ludzki jest najczęstszą przyczyną wycieków danych.

Anna Dmochowska

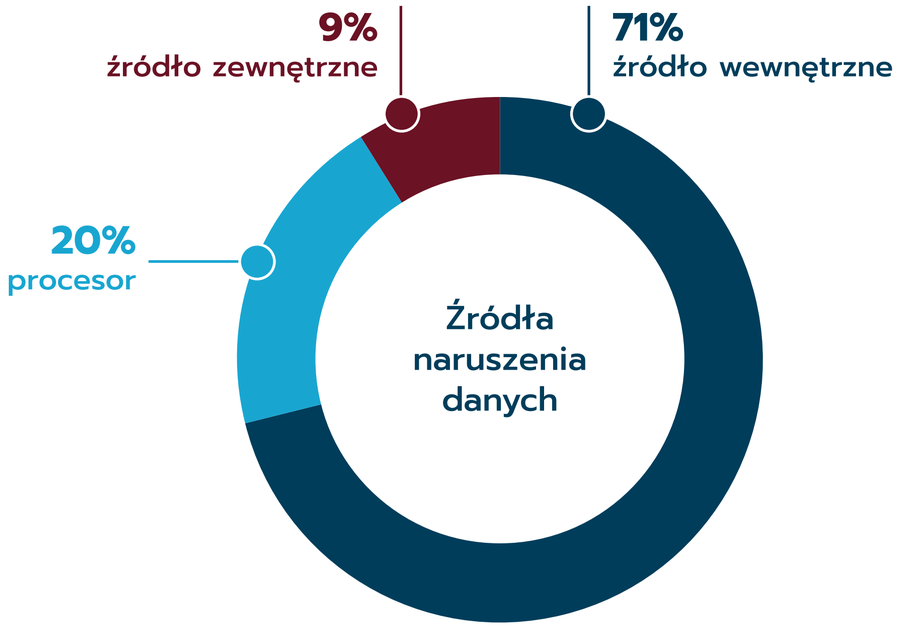
EKSPERT DS. OCHRONY DANYCH ODO 24 SP. Z O.O.

Z przeprowadzonych badań wynika, iż sektor prywatny wygenerował aż 80% wszystkich incydentów odnotowanych przez ZFODO. Wynika to jednak przede wszystkim z faktu, iż tego typu organizacji jest na polskim rynku po prostu najwięcej. Uwagę zwraca również sektor podmiotów finansowych. W omawianym sektorze zawsze będziemy niestety mieli do czynienia z większymi lub mniejszymi incydentami bezpieczeństwa, które mogą kwalifikować się jako naruszenia ochrony danych osobowych. Dzieje się to przede wszystkim za sprawą ilości danych osobowych przetwarzanych przez te podmioty oraz dużej liczby procesów z tym powiązanych.

Powyższe wyniki korespondują ze statystykami prezentowanymi przez Prezesa Urzędu Ochrony Danych Osobowych, zgodnie z którymi za lwią część naruszeń odpowiadają podmioty z branży telekomunikacyjnej, ubezpieczeniowej, finansowej oraz służby zdrowia.

05

Źródło naruszeń danych osobowych



Źródła naruszeń zdecydowaliśmy się podzielić na 3 kategorie:

- Zewnętrzne – nie związane bezpośrednio z organizacją: hakerzy, byli pracownicy etc.
- Wewnętrzne – pracownicy i współpracownicy organizacji.
- Procesor – podmioty przetwarzające dane osobowe na zlecenie administratora.

Blisko ¾ wszystkich incydentów zostało spowodowane działaniami pracowników lub współpracowników organizacji.

ZFODO mówi...

Tomasz Osiej

PREZES ZARZĄDU OMNI MODO SP. Z O.O.

Największą negatywną rolę w naruszeniach odgrywa czynnik wewnętrzny. W ponad 70%, za naruszenia odpowiadają pracownicy i współpracownicy. Nie dziwi to nikogo, kto zajmuje się ochroną danych. Nawet najlepsze zabezpieczenia bez świadomości i odpowiedzialności ludzi nie zadziałają. To cenna wskazówka dla wszystkich planujących działania w obszarze ochrony danych.

Maria Lothamer

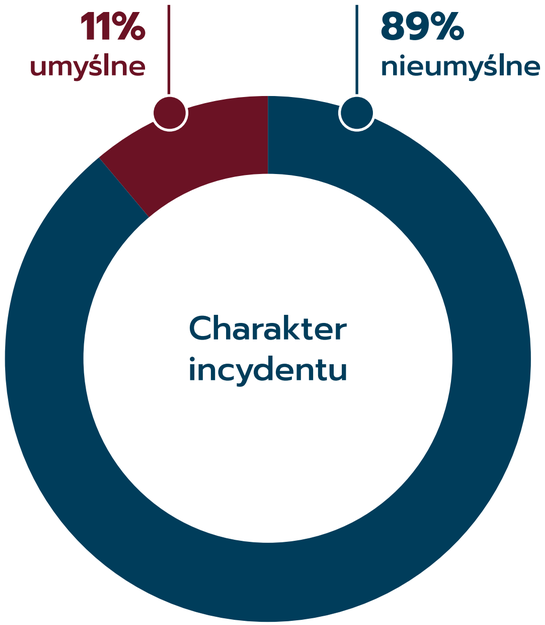
WICEPREZES ZARZĄDU iSECURE SP. Z O.O.

Najczęstsze sytuacje związane z naruszeniami ochrony danych występują wewnątrz organizacji i są powodowane przez pracowników tej organizacji. Nie musi to jednak oznaczać, że ci pracownicy ponoszą pełną odpowiedzialność za spowodowanie naruszenia.

Przy codziennej współpracy z naszymi klientami można zauważyć, że dla niektórych organizacji budżet na odpowiednie środki bezpieczeństwa w postaci np. odpowiednich, zamykanych szaf, oprogramowania zapewniającego bezpieczeństwo urządzeń mobilnych, czy chociażby systematycznych szkoleń pracowników, nie jest kwestią priorytetową. W takim przypadku można powiedzieć, że wina za wystąpienie naruszenia leży po stronie organizacji.

06

Umyślność bądź nieumyślność incydentu



Aż 89% incydentów stanowiły działania nieumyślne. W tej kategorii między innymi:

- błędnie zaadresowane maile,
- brak stosowania kopii ukrytej,
- wysyłka korespondencji tradycyjnej z błędną zawartością (dane osobowe innej osoby).

Wśród działań umyślnych odnotowaliśmy między innymi:

- kradzieże laptopów (lub innych nośników danych),
- różnego rodzaju wyłudzenia informacji,
- udostępnianie danych osobowych osobom nieuprawnionym.

ZFODO mówi...

Przemysław Zegarek

PREZES ZARZĄDU LEX ARTIST SP. Z O.O.

Statystyka pokrywa się z moim subiektywnym odczuciem i doświadczeniem. Umyślne działania hakerskie, wyłudzenia informacji czy kradzieże są bardzo medialne i dużo się o nich mówi, ale to zdecydowana mniejszość. Nie zmienia to faktu, że te 11% umyślnych działań może powodować ogromne szkody dla organizacji.

Działania nieumyślne bywają często bagatelizowane. Trudno w konkretny sposób się przed nimi zabezpieczyć. Nie ma tutaj dróg na skróty. Jedyny skuteczny środek zapobiegawczy to ciężka praca nad przestrzeganiem i egzekwowaniem procedur RODO.

adw. Konrad Wysocki

JDS CONSULTING SP. Z O.O. SP. K.

Przeważająca większość incydentów nie stanowiła wyniku umyślnego działania osób odpowiedzialnych za ich wystąpienie. Incydenty były spowodowane przede wszystkim konsekwencją niedbalstwa lub lekkomyślności, które wynikały z nadmiaru obowiązków służbowych, bądź niedoskonałości procedur.

Administratorzy danych są zatem zobowiązani do przywiązywania nieustannej dbałości o systemy służące do przetwarzania danych, gdyż nawet oczywisty brak winy nie zawsze będzie przesądzał o braku odpowiedzialności za działania osób trzecich względem administratorów.

Należy więc kłaść nieustanny nacisk na uświadamianie o występujących zagrożeniach i szkolenie personelu, celem podnoszenia świadomości prawnej oraz sprawności przekazywania informacji o zaistniałych incydentach, aby zapobiegać ich występowaniu w przyszłości.

07

Przyczyny osobowe vs przyczyny nieosobowe

- **Do przyczyn osobowych zaliczyliśmy działania tzw. czynnika ludzkiego. A więc zarówno działania umyślne zewnętrznych osób (np. hakerów), jak i niezawinione pomyłki pracowników organizacji.**

Przyczyny nieosobowe to sytuacje, kiedy naruszenie spowodowane było błędnym działaniem technologii, sytuacjami niezależnymi od ludzkiej woli.

adw. Konrad Wysocki

JDS CONSULTING SP. Z O.O. SP. K.

Czynnik ludzki jest najczęstszą przyczyną występowania incydentów. Istotna część zdarzeń była wynikiem pracy osób upoważnionych do przetwarzania danych osobowych. Przeprowadzanie operacji na danych, niezależnie od stopnia ich złożoności jest zwykle obarczone ryzykiem, którego poziom kształtuje się w zależności od rodzaju przetwarzanych danych i czynności wykonywanych w ramach obowiązków służbowych.

Do incydentów niezależnych od ludzkiej woli można zaliczyć przede wszystkim awarie systemów informatycznych lub błędne działanie technologii. Należy jednak stanowczo podkreślić, że czynnik ludzki może znacząco przyczynić się do eliminacji nieosobowych źródeł występowania incydentów.

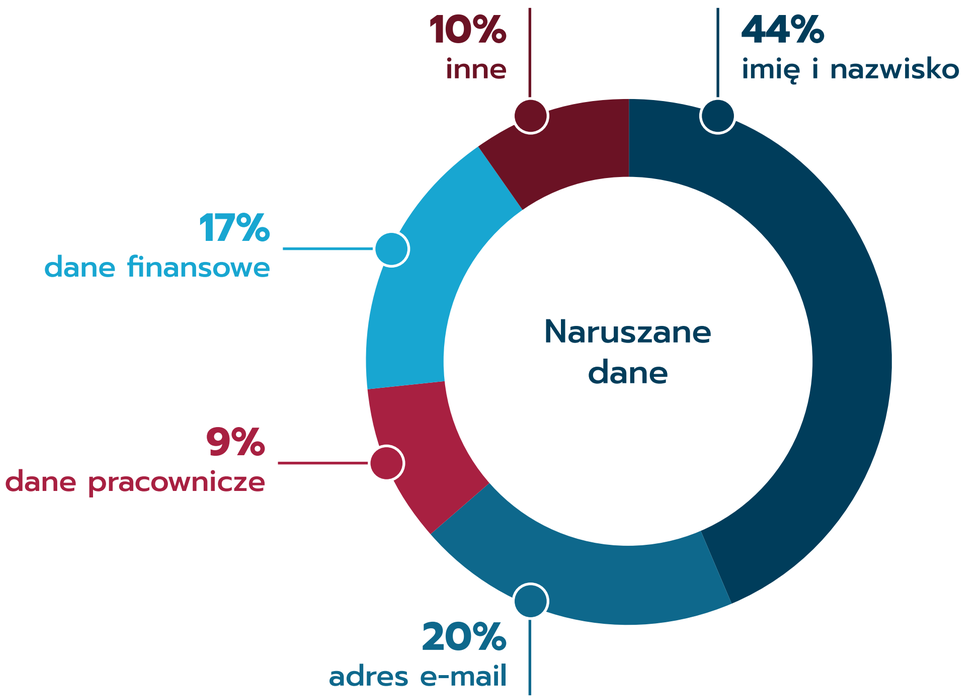
Stałe doskonalenie czynnika ludzkiego może mieć zatem wysoki wpływ na zapobieganie występowania incydentów w przyszłości, w tym także incydentów o podłożu nieosobowym. Podkreślenia wymaga bowiem, że to człowiek stanowi najważniejsze ogniwo w procesie przetwarzania danych osobowych.

adw. Magdalena Jędruchniewicz

ODO MANAGEMENT GROUP SP. Z O.O.

Przetwarzanie danych osobowych jest procesem złożonym. W proces ten zaangażowany jest zarówno czynnik ludzki – pracownicy, współpracownicy przetwarzający dane osobowe jak i pozaludzki – przetwarzanie odbywa się przeważnie za pomocą systemów informatycznych. Naruszenie ochrony danych osobowych może nastąpić zarówno z powodów leżących po stronie personelu (np. nieprzestrzeganie procedur), jak i z przyczyn technicznych (awaria systemu). Zdecydowana większość incydentów (89 %) z jakimi zmierzyliśmy się u naszych klientów ma źródło w działaniach ludzkich i zazwyczaj wynika z błędnych, nieumyślnych działań, a nie świadomego podejmowania czynności prowadzących do incydentu ochrony danych osobowych. Niezależnie od przyczyn zaistnienia naruszenia, każdy przypadek należy wnikliwie przeanalizować i zdecydować czy incydent należy zgłosić organowi nadzorczemu (Prezes Urzędu Ochrony Danych Osobowych), czy o incydencie należy zawiadomić osoby, których dane osobowe zostały naruszone a także jakie środki zaradcze i naprawcze należy przedsięwziąć w celu zapobiegnięcia skutkom incydentu, do którego doszło i uniknięcia powstania naruszeń w przyszłości.

08 Najczęściej naruszane kategorie danych



- **Wykres wskazuje na kategorie danych osobowych, których najczęściej dotyczy naruszenie.**

Na dokonany w ten sposób podział kategorii wpływ miał faktyczny zakres danych, który został ujawniony w protokołach ze stwierdzonych naruszeń. Wskazane kategorie danych zostały podzielone i zsumowane tak, aby wyodrębnić te z nich, które padają ofiarą incydentów najczęściej.

ZFODO mówi...

Tomasz Osiej

PREZES ZARZĄDU OMNI MODO SP. Z O.O.

Wydawało by się, że najczęstszą „ofiarą" naruszeń padają dane służące do logowania, ale tak nie jest. 44% naruszeń dotyczy imienia i nazwiska, następny w kolejności jest adres e-mail (20%). Jeśli do tego dodamy dane finansowe (17%) i kadrowe (10%) wyłania nam się obraz tego jakie dane wypływają z organizacji.

Widać wyraźnie, że bardziej chronimy twarde dane kadrowe i finansowe. Na imię i nazwisko w połączeniu z adresem e-mail musimy zwracać większą uwagę, bo wyciek tych danych także potrafi być „bolesny" z punktu widzenia osoby, której dane wyciekły.

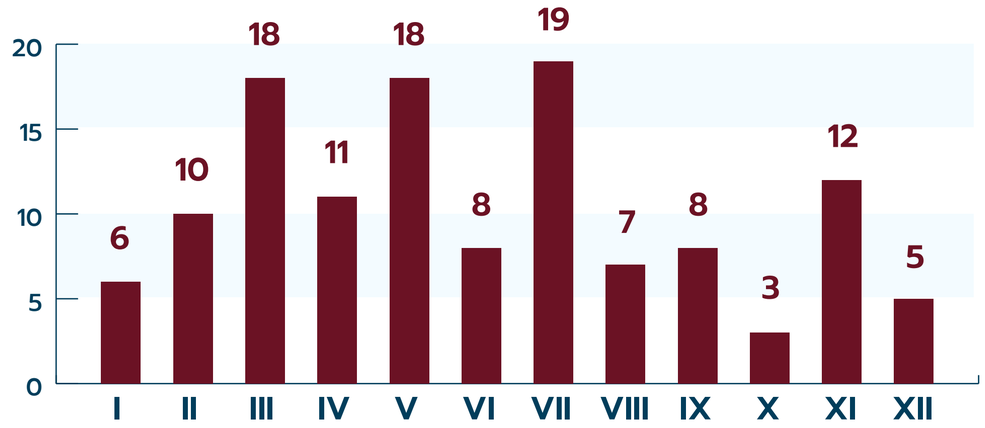
Paweł Latkowski

PARTNER DISCRETIA SP. Z O.O.

Szczęśliwie dla ankietowanych firm, większość naruszeń dotyczy tzw. danych osobowych zwykłych, takich jak imię, nazwisko czy adres email, do których PUODO nie przykłada szczególnej wagi. Podejście nadzoru jest bardziej surowe, gdy dochodzi do wycieku numerów PESEL lub danych szczególnej kategorii.

Wspomniane kategorie danych powinny zostać objęte przez firmy szczególną ochroną, aby uniknąć nieprzyjemnych konsekwencji w postaci kar administracyjnych, które ostatnio pojawiają się coraz częściej.

09 Trend naruszeń



Trend naruszeń w skali roku

- Wykres obrazuje ilość naruszeń z podziałem na miesiące w których zostały one odnotowane. Cykliczne badanie powtarzane na przestrzeni kilku lat pozwoli na wychwycenie trendów w zakresie ilości naruszeń bądź wskazanie miesięcy najbardziej obfitujących w naruszenia.

ZFODO mówi...

Maciej Kaczmarski

PREZES ZARZĄDU ODO 24 SP. Z O.O.

Patrząc na wyniki badania trudno oprzeć się wrażeniu, że ostatnie miesiące roku 2018 obfitowały w znacznie mniejszą liczbę odnotowanych naruszeń. Z drugiej strony uwagę zwraca wysoki wskaźnik w marcu i maju, czyli miesiącach, w których Prezes UODO nałożył dwie pierwsze kary pieniężne. Z naszej – jako ODO 24 – perspektywy wraz z wydłużającym się stażem stosowania RODO, wzrasta świadomość naszych klientów, dlatego o ile zmniejsza się liczba naruszeń, których źródła można upatrywać w braku wiedzy i doświadczenia osób dopuszczonych do przetwarzania danych, o tyle odnotowuje się więcej naruszeń, które są konsekwencją nieuniknionych błędów ludzkich czy kwestii niezależnych od administratorów – co w mojej opinii świadczy o coraz lepiej funkcjonującym systemie ochrony danych osobowych.

Tomasz Gwara

PARTNER DISCRETIA SP. Z O.O.

W miarę upływu czasu obserwujemy wśród naszych klientów tendencję spadkową co do ilości zgłaszanych naruszeń. W naszej ocenie wynika to z „docierania" się systemów ochrony danych osobowych w przedsiębiorstwach, ulepszania istniejących rozwiązań prewencyjnych i rosnącej świadomości pracowników w tym zakresie. Niemniej jednak nasza próba statystyczna nie jest znacząca. Patrząc na dane można powiedzieć, że przeciętna firma może liczyć na wystąpienie 1 incydentu w okresie 2 lat.

Jeżeli:

- **zatrudniasz min. 3 osoby,**
- **specjalizujesz się w RODO min. 5 lat,**
- **Twoja firma prezentuje wysoki poziom merytoryczny i wysokie standardy etyczne,**
- **chcesz współtworzyć podobne raporty,**
- **szukasz kontaktu z praktykami z branży.**

Zapraszamy Cię do naszej organizacji:
www.zfodo.org.pl

Polecamy również zapoznanie się ze stanowiskami i opiniami ZFODO:
www.zfodo.org.pl/opinie/
Odpowiadamy w nich na praktyczne problemy stawiane przez naszych klientów.

ZFODO

Związek Firm Ochrony Danych Osobowych

Ul. Hoża 86/410,
00-682 Warszawa

e-mail: kontakt@zfodo.org.pl
www.zfodo.org.pl