ZFODO

Incydenty ochrony danych osobowych 2020

Raport Związku Firm Ochrony Danych Osobowych

00 O raporcie

- Badaniem objęliśmy **454 organizacje** obsługiwane przez Firmy zrzeszone w ramach ZFODO w okresie **maj 2019–maj 2020**.
- 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.

Partner wspierający

01 Wstęp

Z przyjemnością przedstawiamy Państwu kolejną edycję raportu o incydentach ochrony danych osobowych, którą przygotował Związek Firm Ochrony Danych Osobowych. Ideą przyświecającą stworzeniu niniejszego opracowania, było przybliżenie Państwu kluczowych zagadnień związanych z występowaniem i obsługą incydentów w Polsce.

Raport oparty jest o rzeczywiste dane, dotyczące incydentów obsługiwanych przez profesjonalne firmy działające w branży ochrony danych osobowych, tj. członków ZFODO. Zestawiliśmy wyłącznie dane statystyczne, które zostały uprzednio i całkowicie zanonimizowane, aby zagwarantować, że konkretne przypadki naruszeń nie zostaną zidentyfikowane. Analiza danych statystycznych umożliwia wskazanie trendów, jak zmienia się podejście przedsiębiorców do problemu incydentów. Zapraszamy do zapoznania się ze szczegółowymi wnioskami naszych ekspertów, które znajdują się w treści raportu.

Dane potwierdzają, że ryzyko wystąpienia incydentu dotyczy wszystkich branż. Niezależnie od branży, stałą pozostaje niepewność przedsiębiorców, w jaki sposób należy wykonać obowiązki związane ze stwierdzeniem wystąpienia naruszenia. Wątpliwości te należy przyjąć ze zrozumieniem, bowiem prawidłowe wykonanie zobowiązań wynikających z RODO wymaga specjalistycznej wiedzy, popartej dużym doświadczeniem.

Pozyskanie niezbędnej wiedzy wymusza specjalizację personelu przedsiębiorcy, co zwykle wiąże się z inwestowaniem dużych środków finansowych w tworzenie nowych etatów, np. inspektora ochrony danych. Dodatkowy koszt to poszerzanie wiedzy osoby, której powierzono obsługę incydentów, np. poprzez specjalistyczne i płatne szkolenia.

Pozyskanie odpowiedniego doświadczenia jest bardzo długotrwałe, bowiem incydent nie jest zdarzeniem częstym. Z danych statystycznych wynika, że incydent ma miejsce u przeciętnego administratora statystycznie 0,65 razy w roku, co stanowi ilość niewystarczającą do uzyskania niezbędnej praktyki, tymczasem błąd w obsłudze nawet pojedynczego przypadku, może mieć dla przedsiębiorcy katastrofalne skutki.

Potencjalnym rozwiązaniem powyższych problemów przedsiębiorcy może być wsparcie merytoryczne, którego udzielają podmioty zewnętrzne, działające w formule outsourcingu.

Outsourcing umożliwia łatwy i ekonomiczny dostęp do wysokiej klasy specjalistów, którzy posiadają niezbędne doświadczenie w bieżącej obsłudze naruszeń ochrony danych osobowych. Tylko tacy specjaliści mogą zagwarantować właściwe zrozumienie potrzeb przedsiębiorcy, który poszukuje skutecznych i sprawdzonych rozwiązań, gotowych do uruchomienia w ciągu 72 godzin od stwierdzenia incydentu.

Nie można przy tym zapomnieć, że najlepszym rozwiązaniem jest leczenie przyczyn, a nie objawów – dlatego zalecamy, by odpowiednio wcześniej identyfikować ryzyko biznesowe związane z potencjalnym incydentem. Rozsądny przedsiębiorca powinien zapewnić sobie bieżące wsparcie w dziedzinie ochrony danych, przez odpowiednio wykwalifikowany personel. Wybór, czy takie wsparcie realizować ma zespół wewnętrzny, czy grupa ekspertów świadcząca usługi w ramach outsourcingu, pozostaje indywidualny i uzależniony od czynników biznesowych.

02

Prawdopodobieństwo wystąpienia incydentu

297
odnotowanych incydentów

454
organizacji

0,65
średnia liczba incydentów przypadających na organizację

- **Raportem objęliśmy 454 organizacje, obsługiwane przez 9 różnych firm zrzeszonych w ramach ZFODO w zakresie outsourcingu IOD lub innej stałej współpracy w zakresie ochrony danych osobowych. Łącznie w okresie od 25 maja 2019, do 25 maja 2020, w ww. liczbie organizacji, odnotowano oficjalnie 297 incydentów.**

Daje to średnią 0,65 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.

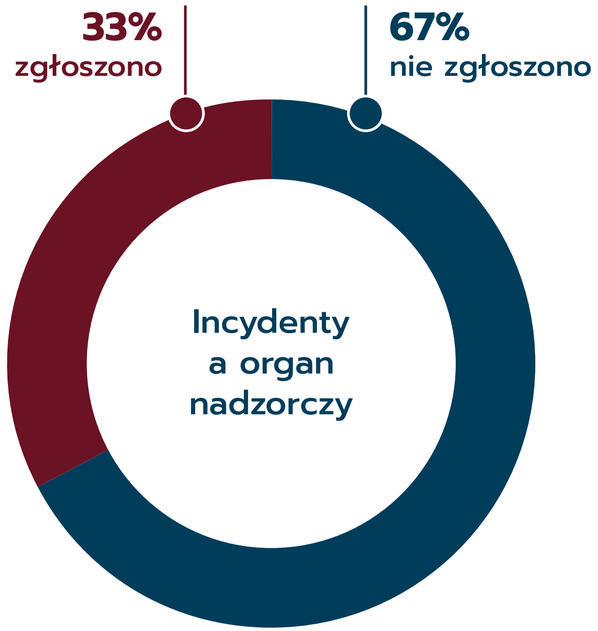
ZFODO mówi...

Tomasz Osiej
PREZES ZARZĄDU OMNI MODO SP. Z O.O.

W porównaniu z poprzednim badaniem (2018 -2019) obecne jest pełniejsze i można powiedzieć, że dojrzalsze. Dojrzalsze dlatego, że samo ZFODO i jego członkowie rozwinęli się w badanym okresie, dzięki czemu dane objęły już nie 277 a 454 organizacji. Ale także dlatego, że rośnie świadomość co do kwalifikowania określonych zdarzeń jako incydenty i konieczności ich zgłaszania. Można powiedzieć, że administratorzy są świadomie od-ważniejsi. To wszystko spowodowało wzrost średniej liczby incydentów przypadających na organizację z 0,46 do 0,65. Patrząc na liczby, skok nie wydaje się może aż tak spektakularny, ale liczby stabilnie rosną.

Okrzepliśmy trochę jako administratorzy danych pod rządami RODO i uczymy się co należy typować jako incydenty, jak je oceniać a finalnie czy i komu zgłaszać. Już w poprzednim raporcie komentując wyniki, przewi-dywaliśmy że wskaźnik incydentów będzie rósł, co odzwierciedliły obecne badania. Czynników wpływających na ten stan jest oczywiście dużo więcej niż sama świado-mość, na pewno można do nich zaliczyć rozwój badanych firm, postępującą digitalizację procesów, zapewne także i trudny czas COVID, który został ujęty w badaniu, ale wzrost świadomości był moim zdaniem decydujący.

03 Incydenty zgłoszone organowi nadzorczemu



- **Blisko 70% incydentów, nie zostało zgłoszonych do organu nadzorczego. Zgodnie z art. 33 ust. 1 RODO, incydentu możemy nie zgłaszać organowi nadzorczemu, 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. Dla porównania, w badaniu sprzed roku do organu nadzorczego nie zgłoszono 59% incydentów.

ZFODO mówi...

Maciej Kaczmarski
PREZES ZARZĄDU ODO 24 SP. Z O.O.

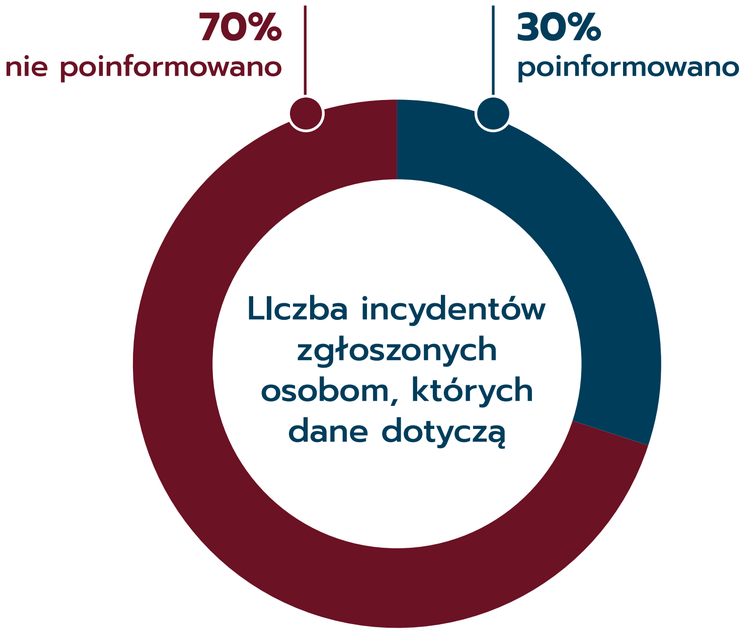
Najnowsze dane wskazują wzrostową tendencję incydentów, które nie zostały zgłoszone organowi nadzorczemu Każdy przypadek wymaga indywidualnej i rzetelnej analizy, niemniej jednak administratorzy powinni mieć świadomość, że decyzja o braku zgłoszenia incydentu może być ryzykowna w dłuższej perspektywie.

Kluczową kwestią jest prawidłowe zidentyfikowanie sytuacji, w której zgłoszenie jest najlepszym rozwiązaniem. Następnym krokiem jest właściwe zorganizowanie samego procesu zgłoszenia. Proces ten wymaga zaangażowania ekspertów w dziedzinie prawa, którzy przygotują dokumentację oraz formularze zgłoszeniowe. W większości przypadków niezbędny będzie także udział ekspertów w dziedzinie IT, którzy zapewnią wdrożenie środków bezpieczeństwa minimalizujących ryzyko ponownego wystąpienia naruszenia, a także pomogą w tym zakresie przeprowadzić analizę ryzyka, która udokumentuje prawidłowość wyboru wdrożonych rozwiązań.

Administrator zgłaszający incydent działa pod presją czasu (72h), a wtedy nie jest trudno o omyłkę: np. zbyt lakoniczny opis zdarzenia, pobieżne wskazanie konsekwencji dla osób dotkniętych incydentem lub błędny szacunek prawdopodobieństwa naruszenia ich praw i wolności. Konsekwencją takich błędów mogą być, dla przykładu, dalsze czynności wyjaśniające Prezesa UODO.

04

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 poprzednim badaniu o incydencie nie poinformowano w 76% przypadków.

ZFODO mówi...

adw. Konrad Wysocki
JDS CONSULTING SP. Z O.O. SP. K.

Stwierdzenie naruszenia ochrony danych przez administratora nie prowadzi wyłącznie bezpośrednio do konsekwencji związanych z możliwością wymierzenia kary administracyjnej przez organ nadzoru. W przypadku zaistnienia incydentu RODO nakłada na przetwarzających dane dodatkowe obowiązki notyfikacyjne, praktycznie nieznane innym aktom prawnym występującym w powszechnie obowiązującym prawie europejskim.

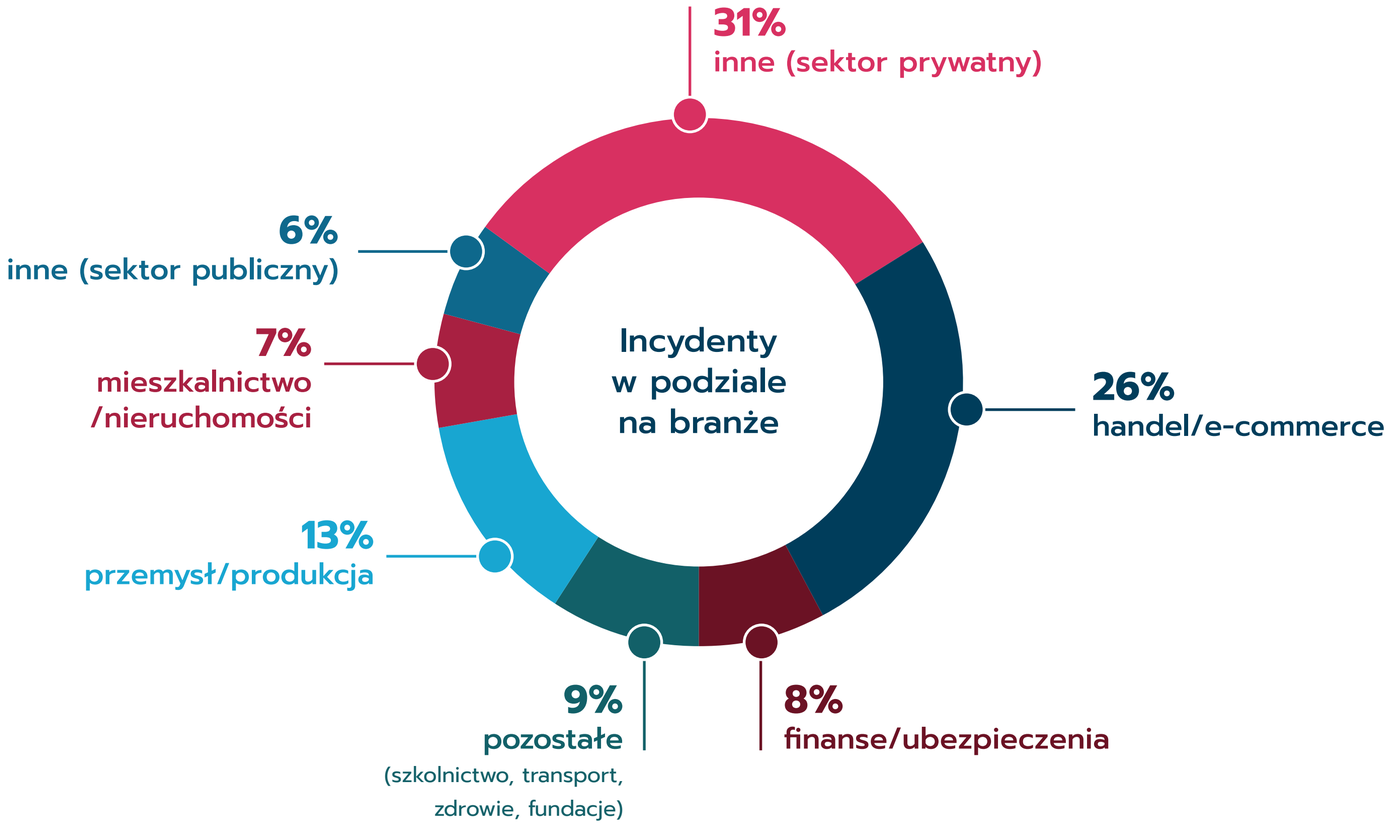
Zaistnienie naruszenia wiąże się zwykle z łącznym wystąpieniem trzech przesłanek:

1) naruszenie musi dotyczyć danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez podmiot, którego dotyczy naruszenie,
2) skutkiem naruszenia może być zniszczenie, utracenie, zmodyfikowania, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych,
3) naruszenie jest skutkiem złamania zasad bezpieczeństwa danych. Każdy administrator danych ma obowiązek zgłosić naruszenie organowi nadzoru bez zbędnej zwłoki, w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, chyba że administrator jest w stanie wykazać zgodnie z zasadą rozliczalności, że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Elementem, który umożliwia właściwe zarządzanie incydentami i ich ocenę jest świadomość prawna w danej organizacji, o której rozwój powinien dbać wyznaczony Inspektor Ochrony Danych.

05

Branże najbardziej narażone na ryzyko naruszeń ochrony danych osobowych



- **Sektor prywatny wygenerował zdecydowaną większość 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 35% wszystkich incydentów (poprzednio 30%).

ZFODO mówi...

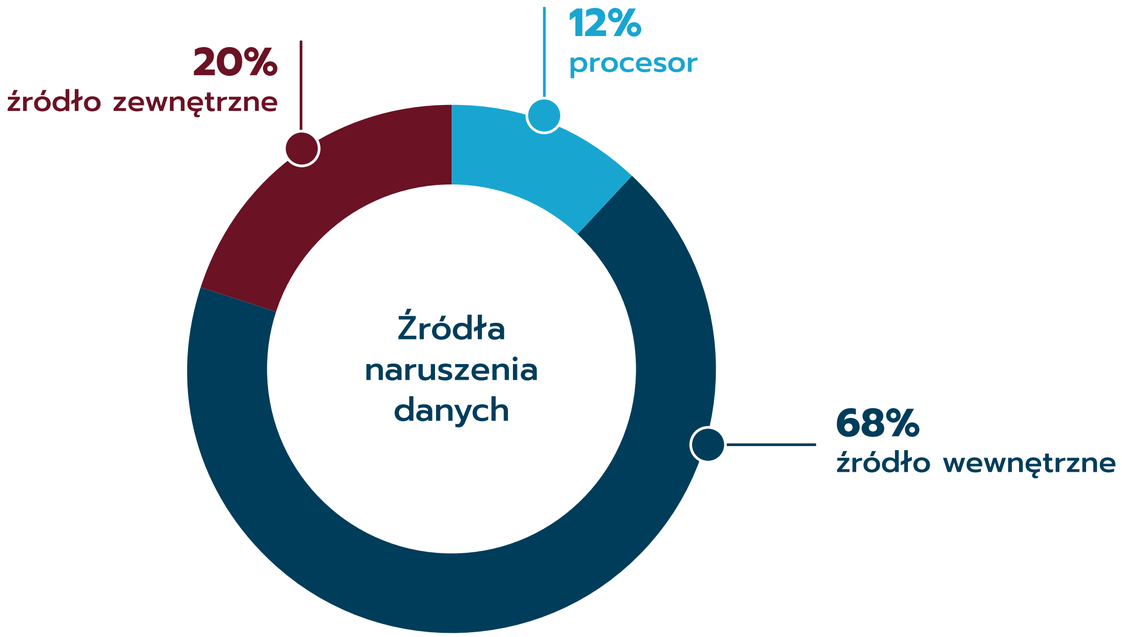
Piotr Kawczyński
DYREKTOR ZARZĄDZAJĄCY, FORSAFE SP. Z O.O.

W analizowanym okresie obserwowaliśmy wzrost liczby incydentów w sektorze prywatnym ze szczególnym udziałem podmiotów specjalizujących się w handlu elektronicznym co przypuszczalnie mogło być związane z konsekwencjami wynikającymi ze sprawy Spółki morele.net. Administratorzy z tego sektora zgłaszali naruszenia – zarówno te kwalifikujące się bezspornie jak i te, których ocena balansowała na granicy wyniku decydującego o notyfikacji w PUODO. Mogło to wynikać ze strachu przed karami ale w mojej ocenie, w większości przypadków podstawowym argumentem decydującym o notyfikacji była niezależna ocena przez organ i pozostawienie decyzji Prezesowi UODO.

W pozostałej części sektora prywatnego przeważająca liczba incydentów oraz naruszeń była związana z utratą poufności danych poprzez nieuprawnione udostępnienie danych osobowych – źródłem tych zachowań były błędy systemowe i niezamierzone działanie człowieka

06

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.

Zdecydowana większość incydentów została spowodowanych działaniami pracowników lub współpracowników organizacji.

ZFODO mówi...

Michał Geilke

INSPEKTOR OCHRONY DANYCH/WŁAŚCICIEL ORLECCY-BEZPIECZEŃSTWO I EDUKACJA

Oczywista dziś uwaga Kevina Mitnicka, że „Człowiek jest najsłabszym ogniwem w łańcuchu bezpieczeństwa" w dalszym ciągu pozostaje olbrzymią bolączką wszystkich procesów przetwarzania danych osobowych. Co więcej, podobno nie mylą się tylko osoby, które nic nie robią. W pracy jesteśmy bowiem po to, aby wykonać konkretny rodzaj zlecenia czy zadania. Jeśli zadanie wiąże się z przetwarzaniem danych osobowych, ryzyko popełnienia błędu, który będzie niósł za sobą poważne konsekwencje dla całej organizacji, niestety wzrasta.

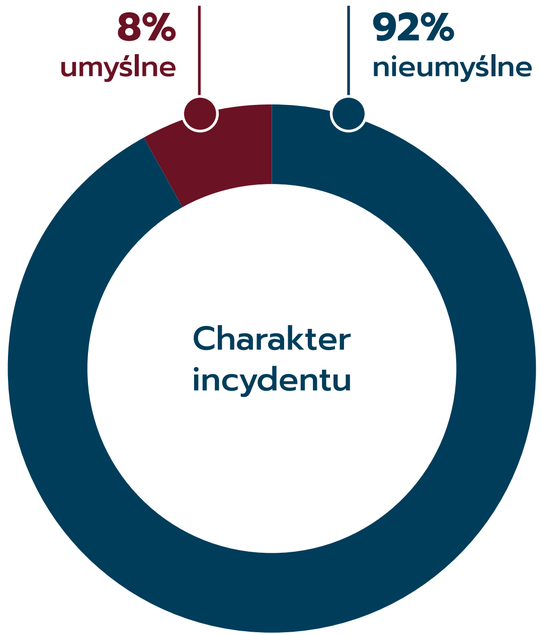
Administrator danych co prawda decyduje o celach i sposobach przetwarzania danych osobowych, ale faktycznie te czynności wykonuje konkretny pracownik lub podwykonawca. Z kolei za błąd pracownika lub podwykonawcy w pierwszej kolejności, co do zasady, odpowiada Administrator danych. Wskazane zależności determinują, w naszej ocenie, fakt, że większość zagrożeń i incydentów ma charakter osobowy - ich źródłem są pracownicy, najczęściej samego administratora danych.

Dlatego istotnym elementem bezpieczeństwa jest budowanie świadomości pracowników i podwykonawców na temat kategorii danych osobowych, z jakimi pracują oraz zagrożeń i ryzyk, jakie się z nimi wiążą.

Ryzyka takie można minimalizować, w szczególności poprzez odpowiednie szkolenia, ale także odpowiednie zaplanowanie dnia pracy (pośpiech jest bardzo złym doradcą) czy stworzenie odpowiednich zapisów w umowach z pracownikami i podwykonawcami.

07

Umyślność bądź nieumyślność incydentu



Aż 92% 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...

Michał Sztąberek
PREZES ZARZĄDU iSECURE SP. Z O.O.

Szczerze powiedziawszy nie jestem zdziwiony tym, że zdecydowana większość incydentów ochrony danych miała charakter nieumyślny. Z moich doświadczeń wynika, że najczęściej problemem jest... wysyłanie e-maili. To właśnie tego typu wiadomości zawierające dane (czy to w treści e-maila czy w postaci załącznika) wysyłane są do błędnych adresatów, a zatem dochodzi do naruszenia poufności danych. To co pozytywne, o ile można tak powiedzieć, to świadomość pracownika, że tego typu sytuacja musi być zgłoszona do IOD w organizacji, by ten mógł dalej nadać sprawie odpowiedni bieg (środki zaradcze – w porozumieniu z kadrą zarządzającą, zgłoszenie do UODO/osób zainteresowanych – gdy jest to konieczne z uwagi na ryzyko naruszenia praw i wolności). Niestety największy problem jest ze środkami zaradczymi minimalizującymi ryzyko wystąpienia incydentu w przyszłości. Kolejne szkolenie może nie być już tak efektywne, choć oczywiście – zawsze warto i należy je przeprowadzić (najlepiej, gdy tylko koncentruje się na naruszeniach – i to takich, które wystąpiły w organizacji – wówczas jest szansa, że w przyszłości pracownicy będą ostrożniejsi).

Zachęcam też organizacje do zainteresowania się narzędziami wspierającymi zapobieganie tego typu naruszeniom. Tylko połączenie procedur, szkoleń i środków technicznych może sprawić, że problem ten zostanie – może nie wyeliminowany w całości – jednak mocno ograniczony.

08

Przyczyny osobowe vs przyczyny nieosobowe

- **Do przyczyn osobowy zaliczyliśmy działania tzw. Czynnika ludzkiego. A więc zarówno działania umyślne zewnętrznych osób (np. hakerów), jak i niezawinionych pomyłek pracowników Organizacji.**

Przyczyny nieosobowe to sytuacje, kiedy naruszenie spowodowane było błędnym działaniem technologii, sytuacjami niezależnymi od ludzkiej woli.
W poprzednim badaniu rozkład przedstawiał się następująco 89% - przyczyny osobowe, 11% - przyczyny nieosobowe.

ZFODO mówi...

Przemysław Zegarek
PREZES ZARZĄDU LEX ARTIST SP. Z O.O.

Wynik badania to przestroga dla wszystkich, wierzących w to, że nowe technologie zabezpieczą w sposób bezobsługowy, posiadane przez nas informacje. Praca z ludźmi jest żmudna, wymaga systematyczności i konsekwencji. I nie gwarantuje sukcesu. Jednak to jedyna droga do wyeliminowania aż 96% naruszeń, które miały miejsce w badanych organizacjach!

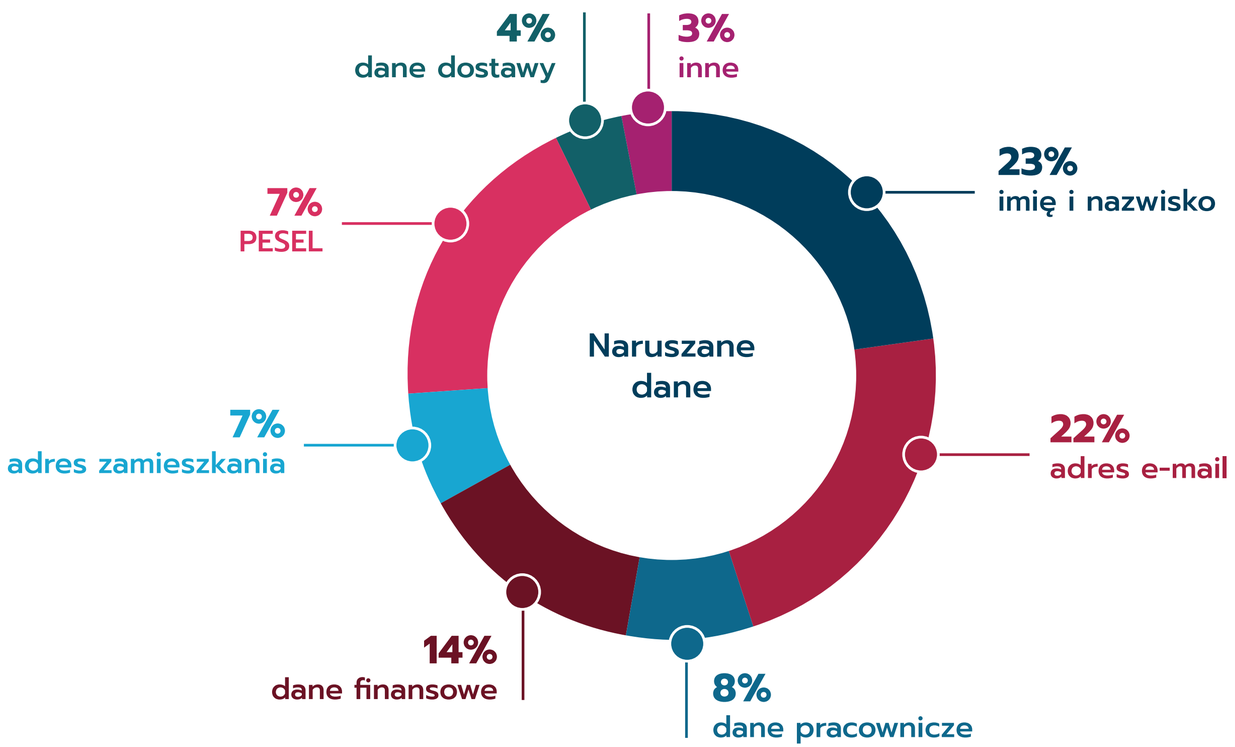
Wciąż uczymy się pracy z ludźmi. Udoskonalamy szkolenia, tworzymy narzędzia diagnozujące poziom RODO świadomości. Kiedy patrzę wstecz na nasze podejście do realizacji szkoleń czy współpracy z ludźmi sprzed 5 czy 10 lat, widzę ogromną zmianę i postęp.

Technologia w porównaniu do czynnika ludzkiego, zawodzi bardzo rzadko.

Klucz do bezpieczeństwa tkwi w umiejętnej pracy z ludźmi, wspartej najlepszą technologią.

09

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...

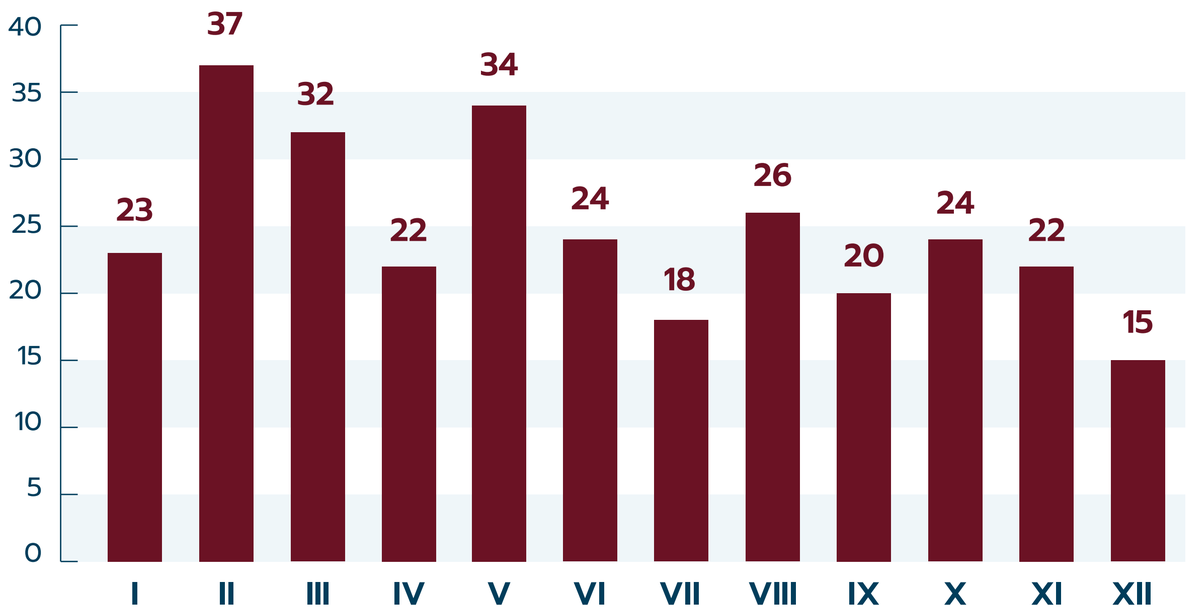
Magdalena Chmielewska
PREZES ZARZĄDU ODO MANAGEMENT GROUP SP. Z O.O.

Na gruncie RODO odróżnić należy dwie kategorie danych osobowych: dane osobowe zwykłe (przetwarzane na podstawach wskazanych w art. 6 ust. 1 RODO) oraz dane szczególnych kategorii (przetwarzane na podstawach wskazanych w art. 9 ust. 2 RODO). Przetwarzanie danych osobowych szczególnych kategorii (np. danych dotyczących stanu zdrowia) wiąże się z koniecznością spełnienia innych - wyższych wymagań w zakresie zapewnienia ochrony tych danych, a każde ich naruszenie może powodować poważne ryzyko naruszenia podstawowych praw i wolności osób, których te dane dotyczą.

Zidentyfikowane na przełomie 2019 i 2020 roku naruszenia ochrony danych osobowych – tak jak w roku poprzednim (maj 2018- maj 2019) - najczęściej dotyczą danych osobowych zwykłych tj. imienia i nazwiska (23%) czy e-maila (22 %). Aż w 20 % badanych incydentów doszło do naruszenia związanego z numerem PESEL. Wprawdzie PESEL należy do kategorii danych osobowych zwykłych, jednakże naruszenie poufności tego numeru, w szczególności w zestawieniu z innymi danymi (np. imieniem, nazwiskiem, adresem) rodzi szereg zagrożeń, mogących skutkować np.: wykorzystania tych danych w celu wyłudzenia kredytu, świadczeń, ubezpieczenia lub brakiem realizacji praw obywatelskich.

Skala naruszeń danych finansowych w analizowanym okresie zmniejszyła się do 15 % względem okresu poprzedniego co może wskazywać zarówno na większą świadomość właścicieli tych danych jak i na skuteczniejsze rodzaje stosowanych przez podmioty zabezpieczeń.

10 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...

Tomasz Gwara
DISCRETIA SP. Z O.O. PARTNER, CEO

Podobnie jak w zeszłym roku, większość naruszeń wystąpiła w lecie i wczesną jesienią, po czym nastąpił spadek ich liczby. Czym wytłumaczyć tę cykliczność? Możliwe, że jest ona skorelowana ze wzmożoną aktywnością biznesową firm w drugim i trzecim kwartale roku.

Obserwując dane nasuwa się jednak inny wniosek: ogólna ilość incydentów nie spada oraz nie ma miesiąca, w którym nie raportowano by naruszeń. Oznacza to, że firmy nadal rozwijają swoje kompetencje w zakresie ochrony danych osobowych – nie potrafią jeszcze skutecznie przeciwdziałać naruszeniom, ale przynajmniej lepiej je raportują.

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