Z F O D O

Incydenty ochrony danych osobowych 2023

Raport Związku Firm Ochrony Danych Osobowych

00 O raporcie

- Badaniem objęliśmy **441 organizacji** obsługiwanych przez Firmy zrzeszone w ramach ZFODO w okresie 1/01/2023 - 31/12/2023.
- 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 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 firm 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 statystyczny 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 wielu etatów, np. inspektora danych osobowych. 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 0,92 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, bo 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 wsparcia ma realizować zespół wewnętrzny, czy grupa ekspertów świadcząca usługi w ramach outsourcingu, pozostaje indywidualny i uzależniony od czynników biznesowych.

02

Prawdopodobieństwo wystąpienia incydentu

407
odnotowanych incydentów

441
organizacji

0,92
średni liczba incydentów przypadających na orgnizację

- Badaniem objęliśmy 441 organizacji, obsługiwanych przez 11 różnych firm zrzeszonych w ramach ZFODO w zakresie outsourcingu IOD lub innej stałej współpracy dotyczącej ochrony danych osobowych.
  Łącznie w okresie od 1 stycznia do 31 grudnia 2023 w ww. liczbie organizacji, odnotowano 407 incydentów.

Daje to średnią 0,92 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...

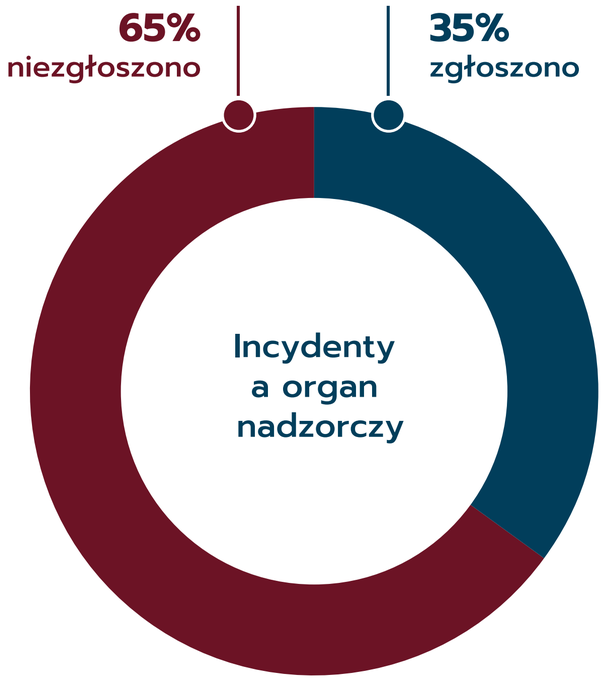
TOMASZ OCHOCKI
WICEPREZES ZARZĄDU ODO 24 SP. Z O.O.

Na podstawie zgromadzonych danych, w ostatnim roku odnotowano spadek średniej liczby incydentów ochrony danych przypadających na organizację – z 1,07 do 0,92 incydentu rocznie. Wynik ten może świadczyć o poprawie efektywności działań prewencyjnych oraz rosnącej świadomości organizacji w zakresie ochrony danych osobowych. Niemniej jednak, liczba 407 odnotowanych incydentów wskazuje, że nadal istnieje potrzeba intensyfikacji działań w zakresie bezpieczeństwa informacji i wzmacniania procedur ochrony danych.

Warto w dalszym ciągu koncentrować się na edukacji pracowników oraz optymalizacji procedur zarządzania ryzykiem, co powinno przyczynić się do dalszego spadku liczby naruszeń w nadchodzących latach.

03

Incydenty zgłoszone Organowi Nadzoru



- 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”

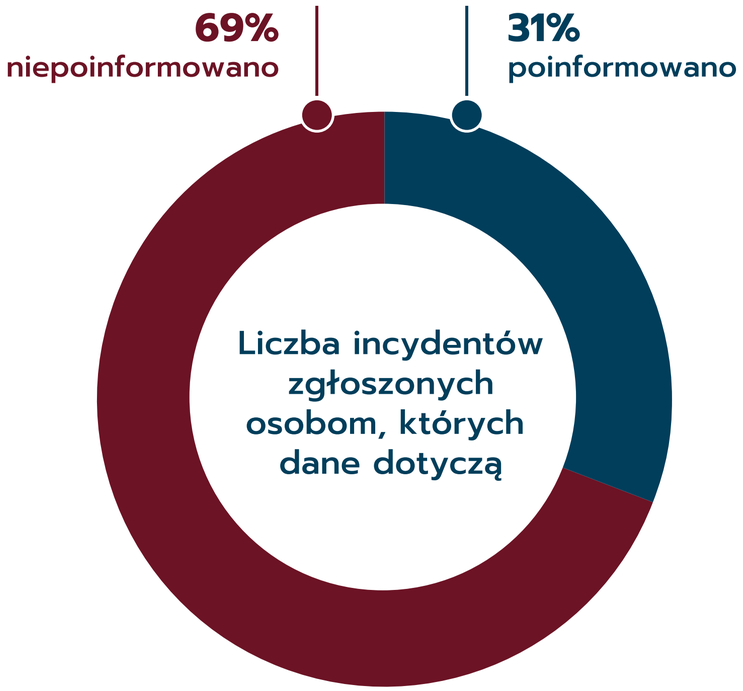
ZFODO mówi...

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

Z całą pewnością można stwierdzić, że ilość zgłaszanych incydentów do organu nadzoru zmniejsza się w porównaniu z tymi pozostającymi w sferze incydentów niepodlegających zgłoszeniu, czyli tych, gdzie nie występuje ryzyko naruszenia praw lub wolności osób, których dane dotyczą. Należy jednak pamiętać, ze ocena wagi naruszenia pozostaje zawsze w gestii administratora. W mojej ocenie od doświadczenia i zasobów, jakimi dysponuje administrator, zależeć będzie prawidłowa jego identyfikacja i dalsze postępowanie z naruszeniem. Warto podkreślić, że administrator analizujący naruszenie działa zawsze pod presją czasu - ustawodawca przewidział na ocenę zgłoszenia 72h. Dlatego też zachęcam, aby dokonując analizy incydentu posiłkować się wiedzą ekspertów zarówno z dziedziny prawa, jak i IT. Kluczowe dla właściwej klasyfikacji naruszenia będzie przeprowadzenie analizy ryzyka, która udokumentuje prawidłowość działania oraz - co niezwykle ważne - udokumentuje zasadność wyboru wdrożonych rozwiań minimalizujących ryzyko ponownego wystąpienia naruszenia.

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 81,51% przypadków.

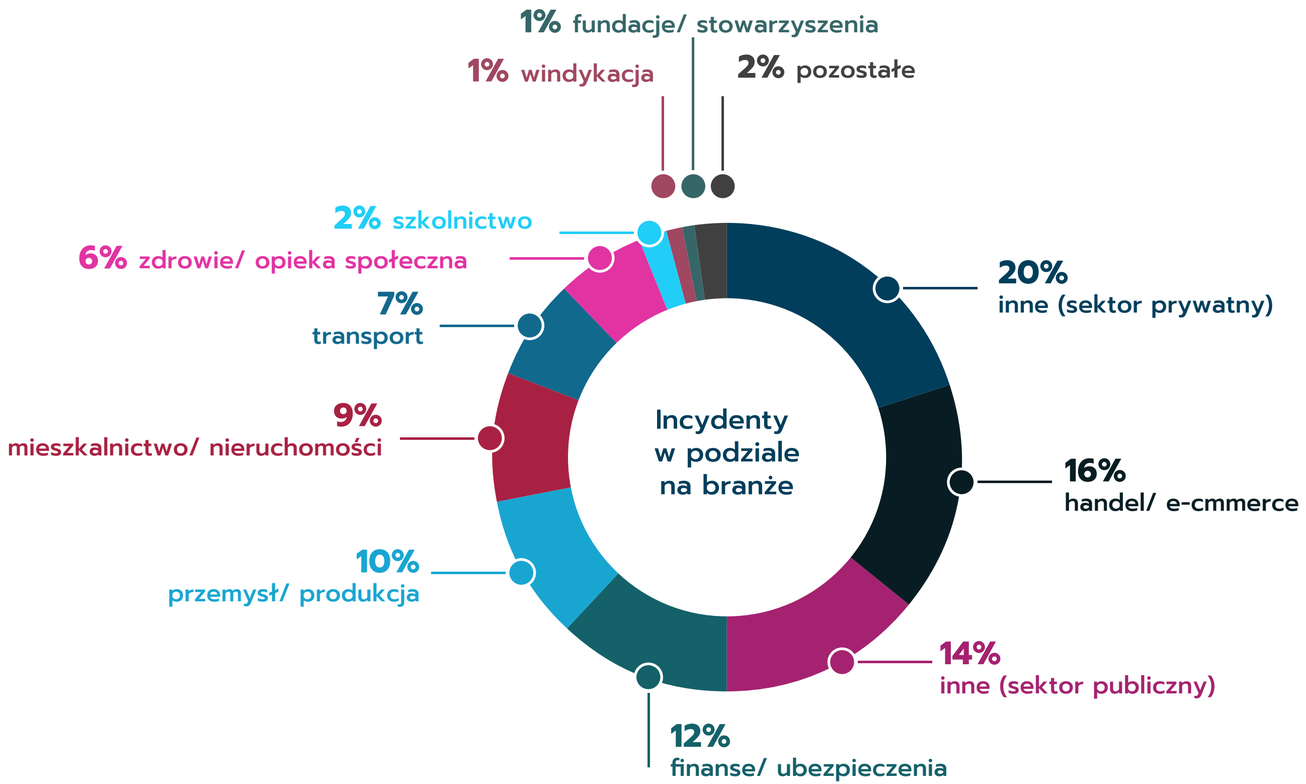
ZFODO mówi...

ALICJA KACZKOWSKA
RADCA PRAWNY, JDS CONSULTING SP. Z O.O. SP. K.

Od 2020 roku obserwowaliśmy tendencję spadkową w zawiadamianiu osób, których dane dotyczą o naruszeniach, natomiast obecnie odnotowujemy znaczny wzrost realizacji tego obowiązku (aż o ponad 12%) w porównaniu z rokiem ubiegłym.
Może to wynikać przede wszystkim z większej ilości incydentów mogących powodować wysokie ryzyko naruszeń praw lub wolności osób, jakie miały miejsce w zeszłym roku. Zauważmy, że w porównaniu z rokiem ubiegłym, znacznie zwiększyła się liczba naruszeń dotyczących takich kategorii danych osobowych, jak nr PESEL czy dane szczególnej kategorii. A, zgodnie z Wytycznymi EROD 9/2022 dotyczącymi zgłaszania naruszenia ochrony danych osobowych na podstawie RODO, kluczowym czynnikiem podczas oceniania ryzyka jest rodzaj i wrażliwość danych osobowych, które zostały narażone w wyniku naruszenia. Zazwyczaj ryzyko powstania szkody dla osób, których dotyczy naruszenie, wzrasta wraz z wrażliwością danych.
Na rosnący odsetek zawiadomień o naruszeniu może mieć również wpływ większa świadomość poszczególnych organizacji na temat konsekwencji, jakie niesie za sobą brak realizacji tego obowiązku wynikającego z art. 34 RODO. Znaczna ilość kar nakładanych przez Prezesa UODO dotyczy obecnie niezgłaszania do Prezesa incydentów, a w konsekwencji niezawiadamiania podmiotów danych o naruszeniach.

05

Branże najbardziej narażone na ryzyko naruszeń ochrony danych osobowych



- Sektor prywatny wygenerował większość incydentów odnotowanych przez ZFODO. Nie można jednak wyciągnąć z tego zbyt daleko idących wniosków. Firmy zrzeszone w ZFODO obsługują w większości sektor prywatny.

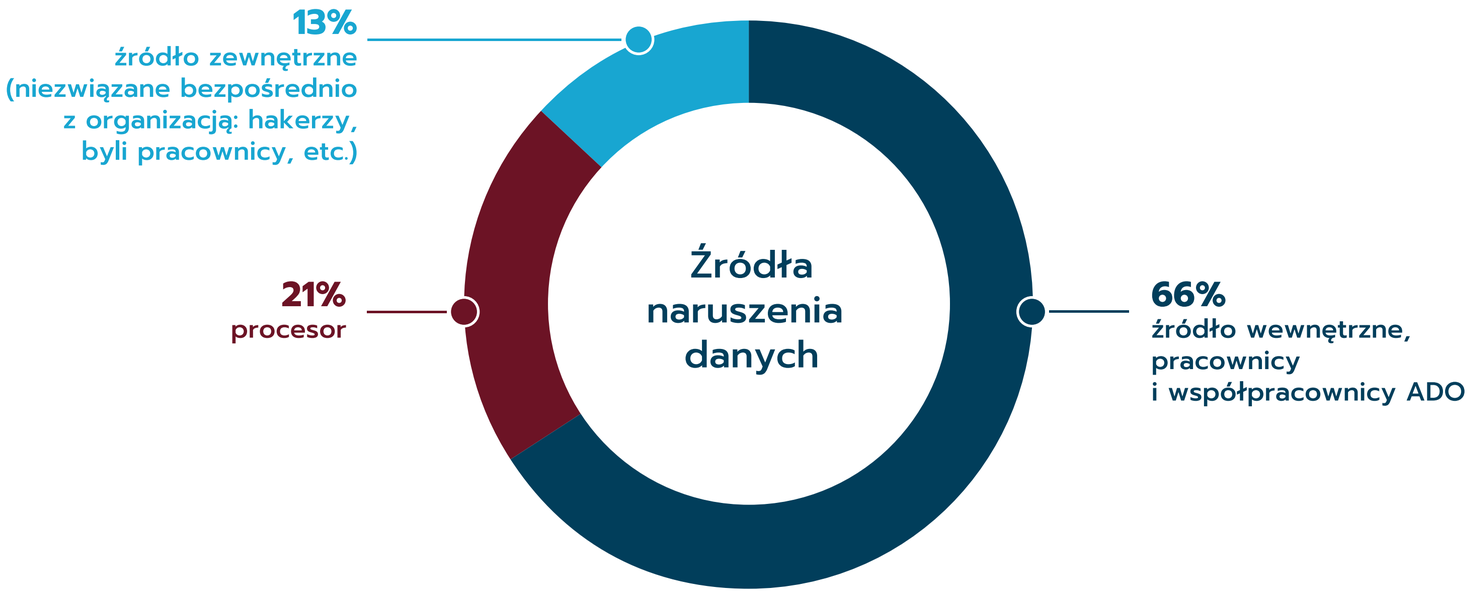
ZFODO mówi...

TOMASZ OSIEJ
PREZES ZARZĄDU OMNI MODO SP. Z O.O.

O ile w latach ubiegłych mieliśmy dosyć przewidywalne wyniki, żeby nie powiedzieć powtarzalne, to w tym roku mamy niespodzianki. Pierwsza z nich to wysoka pozycja, jaką w rankingu zajmuje przemysł/produkcja. Wynika to zapewne z tego, że dopiero teraz profesjonalne firmy zaczęły obsługiwać więcej podmiotów z tego sektora, a to przełożyło się na większa świadomość, a więc także liczbę ujawnionych incydentów. Drugie zaskoczenie, choć nie tak duże jak poprzednie, to wciąż wysokie miejsce jakie zajmuje w rankingu handel i e-commerce. Trzecia niespodzianka to branża zdrowie/opieka społeczna, która na podstawie posiadanych przez nas danych wydaje się niedoszacowana, pomimo tak dużej uwagi skupionej na niej przez organ nadzoru.

06

Źródło naruszeń danych osobowych



- **Źródła naruszeń zdecydowaliśmy się podzielić na 3 kategorie:**
  - Zewnętrzne – niezwiązane 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.

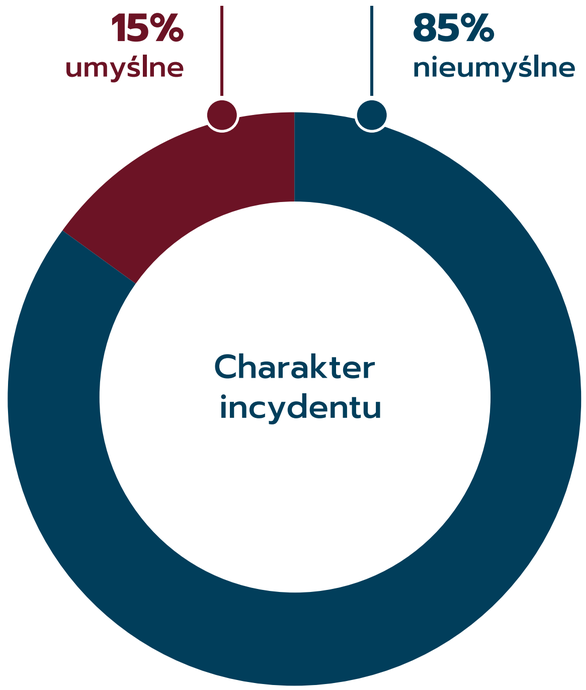
ZFODO mówi...

MAGDALENA CIEŚLAK
RADCA PRAWNY, DISCRETIA SP. Z O.O.

Głównym źródłem naruszeń danych osobowych w organizacjach nadal pozostają pracownicy, czyli czynniki wewnętrzne. Należy jednak zauważyć, że udział naruszeń wewnętrznych znacząco spadł w porównaniu do lat ubiegłych, z poziomu 86,27% w 2022 roku do 66% w 2023 roku. Może to świadczyć o postępach w budowaniu świadomości pracowników oraz poprawie procedur ochrony danych.
Jednocześnie zdecydowanie rośnie ryzyko związane z procesorami oraz zagrożeniami zewnętrznymi, w tym cyberatakami, które stanowią coraz poważniejsze wyzwanie dla organizacji i wymagają szczególnej uwagi.
Prognozy na przyszłość wskazują na konieczność dalszego wzmacniania działań w zakresie cyberbezpieczeństwa oraz lepszej kontroli nad procesorami. Organizacje powinny kontynuować szkolenia pracowników, inwestować w nowe technologie ochrony danych oraz doskonalić procedury reagowania na potencjalne incydenty.
Zrozumienie źródeł naruszeń oraz szybka adaptacja do zmieniających się zagrożeń są kluczowe dla skutecznego zarządzania ochroną danych osobowych.

07

Umyślność bądź nieumyślność incydentu



- **Aż 85% incydentów stanowiły działania nieumyślne (w poprzednim badaniu statystyka wyglądała podobnie: 94,64%). 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

EKSPERT DS. OCHRONY DANYCH OSOBOWYCH, CEO W ISECURE SP. Z O.O.

Nieumyślne naruszenia ochrony danych osobowych, które – jak wskazuje najnowsza edycja raportu – cały czas występują najczęściej, mogą mieć wiele przyczyn, które często wynikają z ludzkich błędów, niedopatrzeń, a także złożoności i szybkości pracy w erze cyfrowej.

Przyczyny te w zasadzie także pozostają niezmienne, a są to: brak świadomości i odpowiednich szkoleń (np. pracownicy nie zawsze są świadomi przepisów dot. ochrony danych osobowych ani nie znają zasad postępowania z nimi), błąd ludzki (w sumie to jeden z najczęstszych powodów występowania tego typu naruszeń, weźmy najprostszy przykład: wysłanie e-maila z danymi osobowymi do niewłaściwego odbiorcy), brak odpowiednich procedur i kontroli (w wielu firmach cały czas brakuje odpowiednich procedur postępowania z danymi osobowymi), niewystarczające zabezpieczenia techniczne (np. brak szyfrowania danych, brak autoryzacji dostępu), problemy z zarządzaniem uprawnieniami (np. pracownik ma szerszy dostęp do danych niż jest mu faktycznie potrzebny do wykonywania obowiązków), posługiwanie się przestarzałym sprzętem i oprogramowaniem (np. nieaktualne systemy operacyjne, nieaktualizowane oprogramowanie, a co za tym idzie potencjalne luki w zabezpieczeniach) oraz presja czasu i stres (można by rzec – oczywista oczywistość, ale dla porządku wspomnę o tym, że w stresujących sytuacjach pracownicy mogą omijać pewne procedury, by szybciej zrealizować zadanie).

Na koniec zostawiłem sobie jeszcze jedną przyczynę, może obecnie nieco mniej popularną, bo część pracowników wróciła już do pracy stacjonarnej, niemniej warto wskazać również pracę zdalną i korzystanie z prywatnych urządzeń. Przykłady: korzystanie z prywatnych, słabiej zabezpieczonych urządzeń, logowanie się przez niezabezpieczone sieci.

Spróbujmy to zatem jakoś zgrabnie podsumować - zapobieganie nieumyślnym naruszeniom wymaga nie tylko odpowiedniego przeszkolenia pracowników i wdrożenia zasad, ale także systematycznego monitorowania oraz stosowania odpowiednich narzędzi i procedur w celu minimalizowania ryzyka błędów.

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 93,13% - przyczyny osobowe, 6,87% - przyczyny nieosobowe.

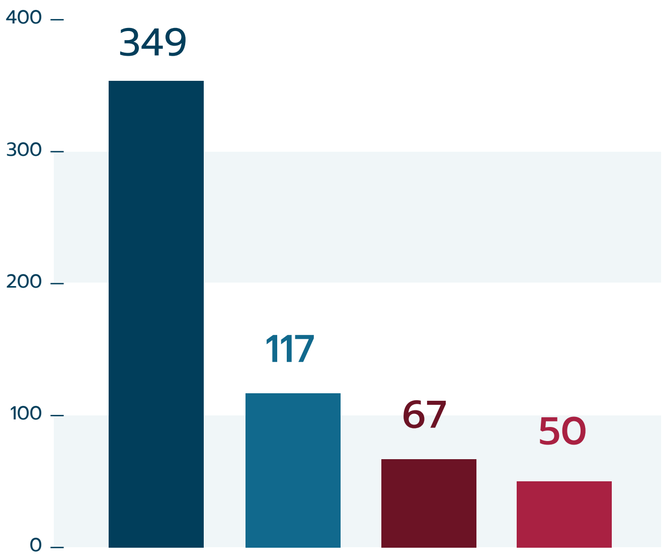
ZFODO mówi...

PIOTR KAWCZYŃSKI
WICEPREZES ZARZĄDU FORSAFE SP. Z O.O.

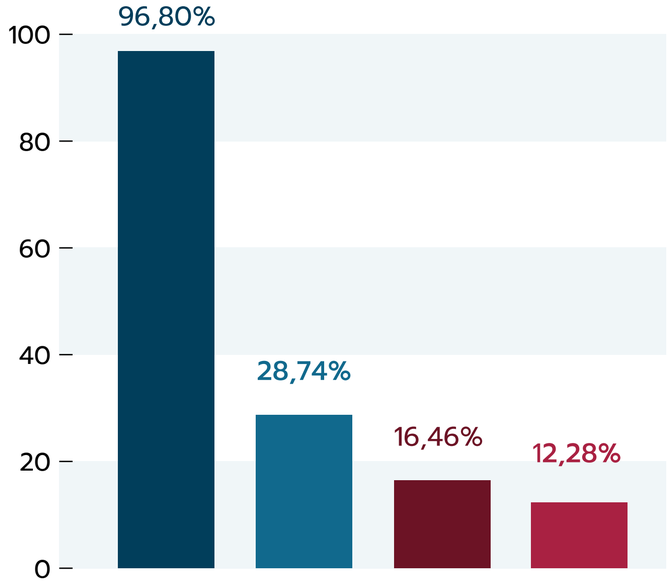
Przyczyny naruszeń mające związek z działaniami człowieka - czy to celowymi czy też przypadkowymi/omyłkowymi - nie są zaskoczeniem w kolejnej edycji raportu. Źródła osobowe stanowią grupę sześciokrotnie większą od źródeł nieosobowych. Jeżeli zestawić to na przykład z masowymi atakami phishingowymi, w których wektorem ataku jest człowiek, a skutkiem najczęściej infekcja oprogramowaniem typu ransomware - łatwo dojść do wniosku, że wszyscy powinni być żywo zainteresowani i skupieni na budowaniu świadomości oraz kultury cyberbezpieczeństwa w swoich organizacjach. Również ze względu na to, że zabezpieczenia informatyczne nie gwarantują kompleksowego bezpieczeństwa, a są jednym z elementów całego systemu.

09 Najczęściej naruszane kategorie danych

Ile incydentów dotyczyło jednej z 4 kategorii danych?



W jakim procencie incydentów, znalazły się dane osobowe poniższych kategorii:



dane podstawowe PESEL dane finansowe dane szczególnej kategorii

* Dane sumują się do więcej niż 100%, ponieważ każdy z 407 incydentów mógł zawierać dane jednej lub większej ilości kategorii.

ZFODO mówi...

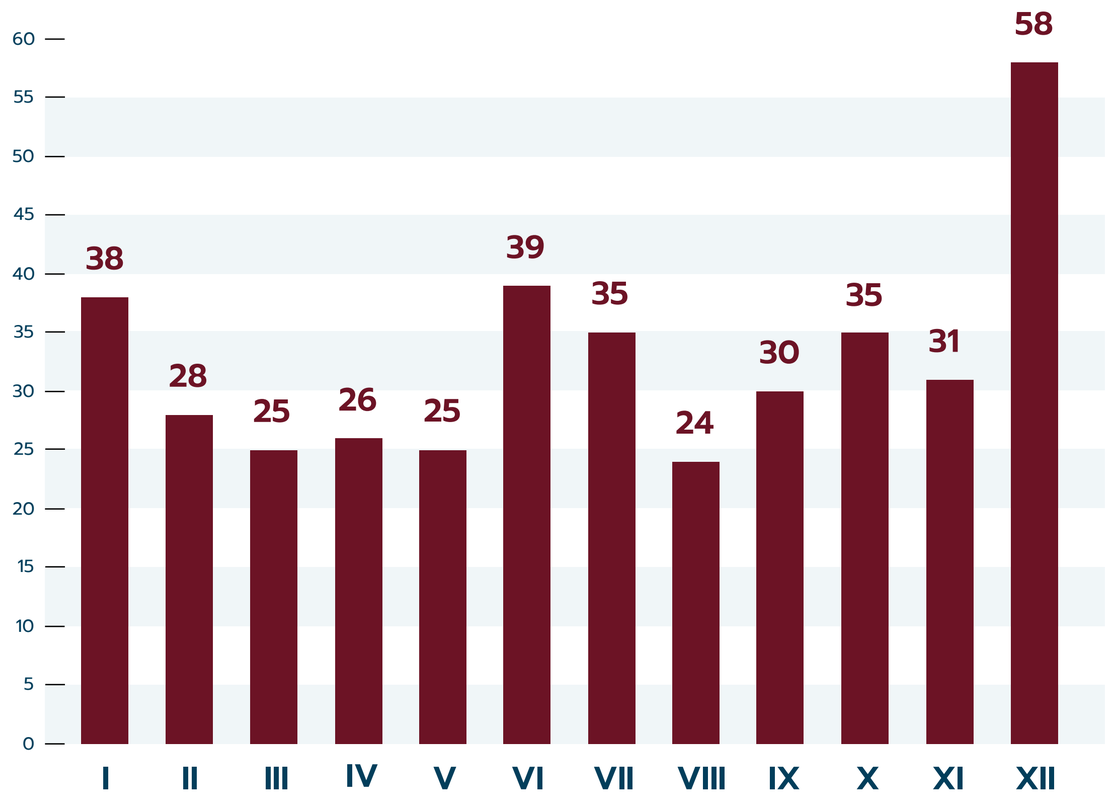
MICHAŁ GEILKE

INSPEKT OCHRONY DANYCH/ WŁAŚCICIEL ORLECCY-BEZPIECZEŃSTWO I EDUKACJA

Podobnie jak w zeszłym roku w aktualnym raporcie wykazujemy, że najwięcej naruszeń dotyczy tzw. „podstawowych danych osobowych" jak np. imię i nazwisko, adres e-mail czy adres zamieszkania/do doręczeń. Wraz z rozwojem technologii i postępującą cyfryzacją coraz więcej usług wymaga od użytkowników podania podstawowych danych osobowych. Robimy zakupy online, korzystamy z mediów społecznościowych, rejestrujemy się na stronach internetowych, załatwiamy sprawy w urzędach, a każda z tych czynności wiąże się z przekazaniem danych. Im więcej miejsc, w których udostępniamy swoje dane, tym większe ryzyko ich wycieku. Użytkownicy powinni być świadomi tego ryzyka i podejmować odpowiednie środki ostrożności, takie jak: ograniczenie liczby serwisów, z których korzystają, wybieranie tylko zaufanych platform, regularne usuwanie kont z nieużywanych serwisów czy stosowanie silnych haseł i uwierzytelniania dwuskładnikowego. Jednocześnie warto zastanowić się, czy rzeczywiście potrzebujemy korzystać z wielu serwisów o tym samym przeznaczeniu – np. sześciu różnych komunikatorów w telefonie.

10

Trend naruszeń



- Wykres obrazuje ilość naruszeń z podziałem na miesiące w których zostały one odnotowane.

ZFODO mówi...

PRZEMYSŁAW ZEGAREK

PREZES ZARZĄDU LEX ARTIST SP. Z O.O.

Podobnie jak w poprzednich latach, nie widzimy wyraźnych trendów w przedstawionej statystyce. Zbieramy dane dotyczące naruszeń z różnych branż. Każda z tych branż może mieć swoje własne miesiące najbardziej obfitujące w naruszenia.

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