ZFODO

Incydenty ochrony danych osobowych 2022

Raport Związku Firm Ochrony Danych Osobowych

00 O raporcie

- Badaniem objęliśmy **435 organizacji** obsługiwanych przez Firmy zrzeszone w ramach ZFODO w okresie **maj 2021 – maj 2022**
- 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 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 0,89 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

466
odnotowanych incydentów

435
organizacji

1,07
średnia liczba incydentów przypadających na organizację

- Badaniem objęliśmy 435 organizacji, obsługiwanych przez 9 różnych firm zrzeszonych w ramach ZFODO w zakresie outsourcingu IOD lub innej stałej współpracy dotyczącej ochrony danych osobowych. Łącznie w okresie od 25 maja 2021, do 25 maja 2022, w ww. liczbie organizacji, odnotowano 466 incydentów.

Daje to średnią 1,07 incydentu rocznie na każdą organizację. Badanie opieramy na incydentach, które zostały zgłoszone firmom zrzeszonym w ZFODO przez obsługiwane przez nich organizacje. Liczbaincydentów, które wystąpiły w rzeczywistości może być wyższa.

ZFODO mówi...

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

Trend rosnącej ilości naruszeń utrzymuje się od samego początku zbierania danych przez ZFODO. W najnowszym raporcie po raz pierwszy odnotowaliśmy ponad jedno naruszenie na organizację w skali roku. Nasze dane są bardziej bezpieczne czy bardziej zagrożone? W mojej opinii wciąż mamy do czynienia z rosnącą wykrywalnością. Naruszenia wcześniej zamiatane pod dywan, są dzisiaj prawidłowo notyfikowane wewnętrznie. Stąd dalszy wzrost średniej naruszeń.

03 Incydenty zgłoszone organowi nadzorczemu

- Ponad 70% 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".

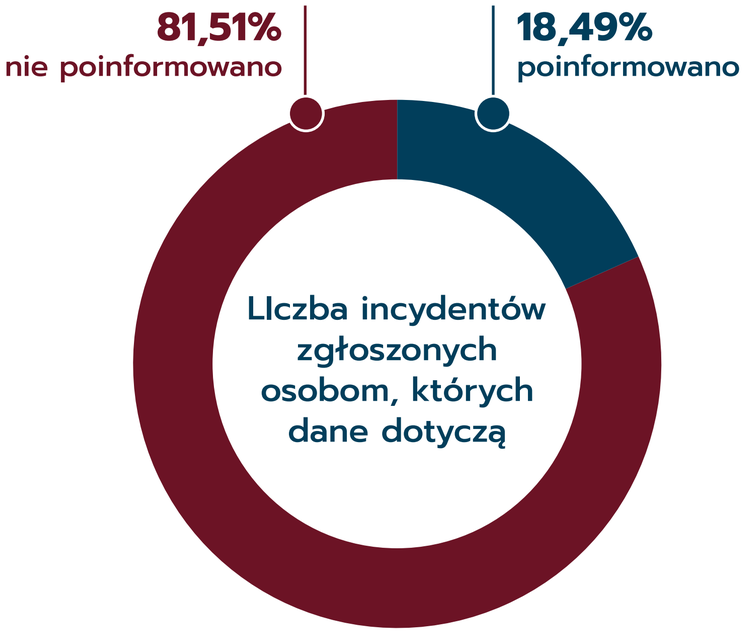
Incydentów jest więcej niż przed rokiem, ale mniejsza ich część jest zgłaszana do Organu Nadzorczego.

ZFODO mówi...

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

Z optymizmem przyglądam się rosnącym wykresom na korzyść incydentów niezgłoszonych. Jeżeli wierzyć statystyce to dane Polek i Polaków stają się coraz bardziej bezpieczne, skoro zgłoszeniu podlegają jedynie incydenty, gdzie występuje większe niż małe prawdopodobieństwo, by zdarzenie skutkowało naruszeniem praw lub wolności osób fizycznych. Oznacza to, że przeważająca większość naruszeń nie stwarzała istotnych problemów, zaś organizacje znalazły sposób, aby sobie z nimi sprawnie poradzić. Dokonanie samodzielnej i skutecznej oceny prawdopodobieństwa naruszenia staje się coraz bardziej powszechne. Rośnie również ilość narzędzi i praktycznych przykładów, które pomagają w zarządzaniu incydentami. Nie twierdzę, że w przyszłości uda się całkowicie wyeliminować incydenty, natomiast gromadzenie rzetelnej wiedzy o naruszeniach sprzyja budowaniu ekosystemów przetwarzania danych domyślnie nastawionych na minimalizację ryzyka. Dla porównania, w badaniu sprzed roku do regulatora zgłoszono 33,01 % z wszystkich naruszeń.

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 75,08% przypadków.

ZFODO mówi...

Tomasz Ochocki
WICEPREZES ZARZĄDU ODO 24 SP. Z O.O.

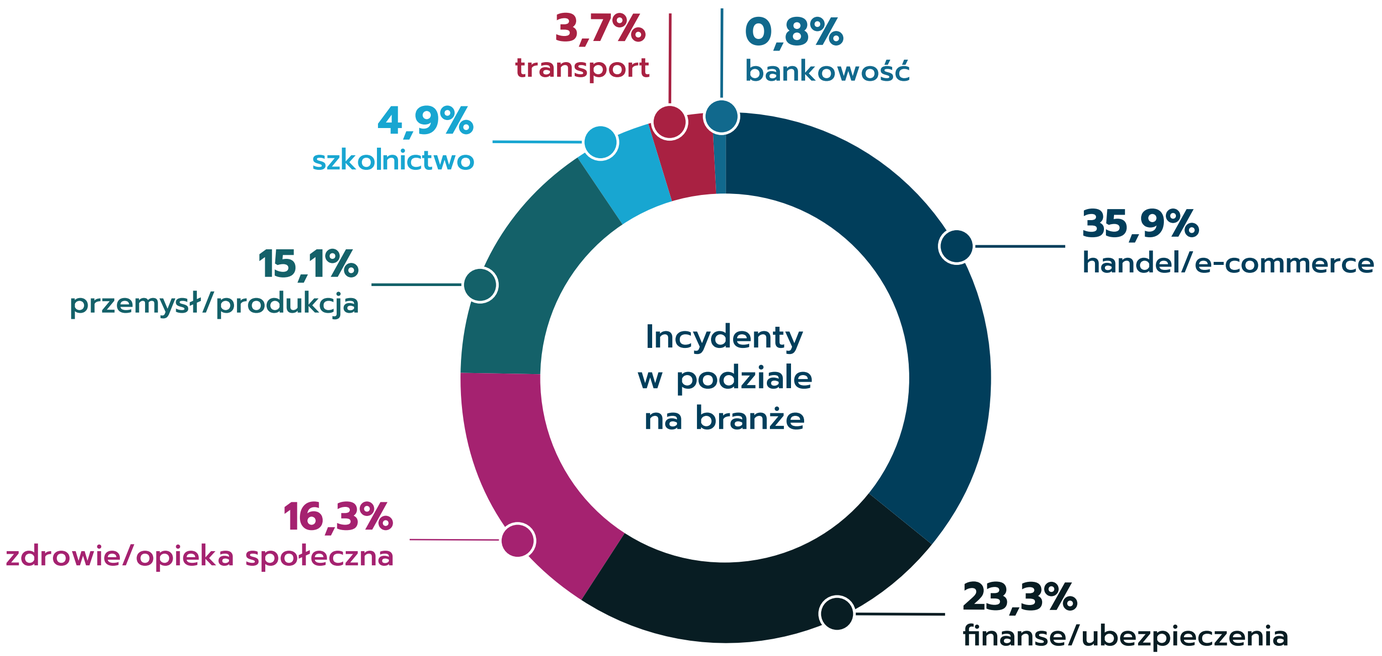
Tegoroczne wyniki badań są dla mnie zastanawiające. Co prawda, odsetek naruszeń, o których zostały poinformowane osoby, których dane dotyczą, spada regularnie od 2020 r., toteż nie można mówić o nagłym załamaniu się realizacji tego obowiązku, natomiast otwarte pozostaje pytanie, dlaczego tak się dzieje.

Możliwym wytłumaczeniem takiego stanu rzeczy mogłoby być zyskiwanie doświadczenia w stosowaniu RODO przez poszczególne organizacje. Nie znajduje ono jednak potwierdzenia w praktyce działania Prezesa UODO. Błędy związane z zarządzaniem naruszeniami ochrony danych (brak zgłoszenia naruszenia do Prezesa UODO, niepoinformowanie osób, których dane dotyczą) były przyczyną 36% kar nałożonych dotychczas przez Prezesa UODO.

Co to oznacza? W mojej opinii, zmniejszająca się liczba naruszeń, o których zostały poinformowane osoby, których dane zostały skompromitowane, pomimo wzrostu ich ogólnej liczby, może świadczyć o większej skłonności polskich organizacji do ryzyka. Być może bardziej obawiają się one szumu medialnego związanego z ujawnieniem informacji o naruszeniu (nieraz kilku tysiącom osób) lub próbą dochodzenia wobec nich zadośćuczynienia niż kary Prezesa UODO.

05

Branże najbardziej narażone na ryzyko naruszeń ochrony danych osobowych



- Sektor prywatny wygenerował znaczącą część 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 34% wszystkich incydentów (poprzednio 59,2%).

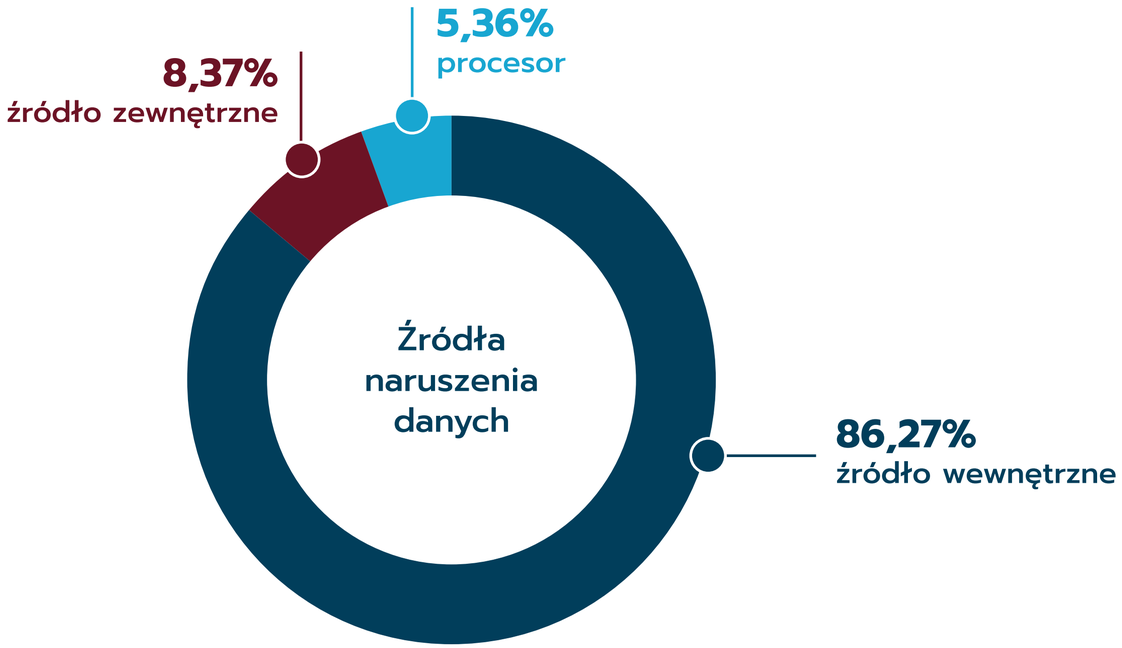
ZFODO mówi...

Piotr Kawczyński
PREZES ZARZĄDU FORSAFE SP. Z O.O.

Wyniki w ujęciu procentowym odnoszącym się do branż najbardziej narażonych na ryzyko naruszeń ochrony danych osobowych dobrze korespondują z planem kontroli Urzędu Ochrony Danych Osobowych na 2023r. Biorąc pod uwagę ryzyka wynikające ze specyfiki przetwarzania oraz zakresu danych podmioty przetwarzające dane osobowe przy użyciu aplikacji internetowych powinny zwrócić szczególną uwagę nie tylko na zaimplementowane zabezpieczenia, ale również na ich skuteczność oraz weryfikację tej skuteczności. Sektor ubezpieczeniowy i finansowy powinien pamiętać o dodatkowych wymaganiach bezpieczeństwa, szczególnie podczas wykorzystywania rozwiązań chmurowych. Natomiast skuteczne ataki na podmioty działające w sektorze ochrony zdrowia pokazały jak wiele do zrobienia jest w kontekście bezpieczeństwa. Podsumowując: testowanie, audytowanie i proaktywność.

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...

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

Tegoroczne wyniki raportu ponownie wskazują, że większość naruszeń ochrony danych osobowych ze względu na źródło pochodzenia naruszenia ma miejsce wewnątrz organizacji. Potwierdza się zatem teoria, że najsłabszym ogniwem w łańcuchu bezpieczeństwa danych jest człowiek.

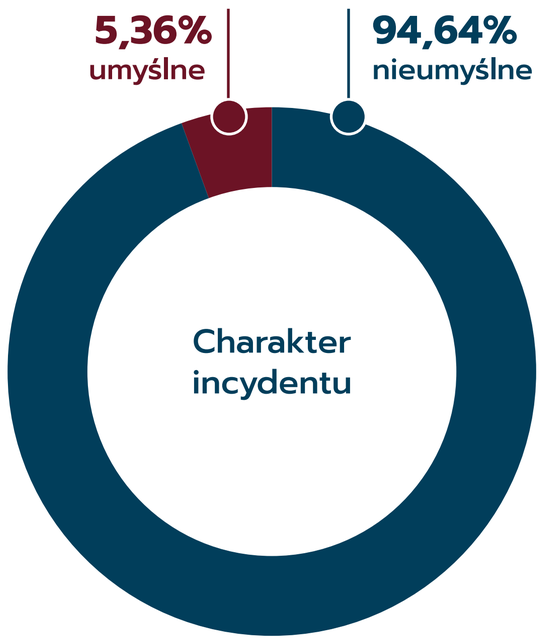
Ze statystyk zebranych przez ZFODO na przestrzeni 4 lat z 1.515 organizacji wynika, że Administratorzy danych nadal nie poradzili sobie z odpowiednim zabezpieczeniem danych przetwarzanych przez ich pracowników i współpracowników, na co wskazuje wciąż rosnący odsetek tych naruszeń, który w roku 2022 osiągnął poziom 86,27%.

Odwrotnie proporcjonalnie niż w powyższym przypadku wyglądają statystyki związane z zabezpieczeniem danych osobowych przekazywanych procesorom; naruszenia ochrony danych osobowych wynikające ze strony podmiotu przetwarzającego dane w imieniu Administratora to średnio ok 10,6% w skali wszystkich naruszeń od momentu wprowadzenia RODO.

Natomiast analiza naruszeń pochodzących z otoczenia organizacji, wskazuje na spadek liczby tego typu zdarzeń począwszy od roku 2020, co uznać należy za potwierdzenie stosowania przez Administratorów lepszych zabezpieczeń infrastruktury informatycznej oraz wykorzystanie bardziej adekwatnych środków organizacyjnych niż w dwóch pierwszych latach stosowania RODO.

07

Umyślność bądź nieumyślność incydentu



- **Aż 94,64% incydentów stanowiły działania nieumyślne (w poprzednim badaniu statystyka wyglądała podobnie: 92%). 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...

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

Kolejna edycja raportu potwierdza to co wszyscy wiemy, a mianowicie fakt, że większość incydentów ma charakter nieumyślny. Ale dopiero to badanie pokazało ile wynosi ta większość, a oscyluje ona od lat na tym samym poziomie, tj. pomiędzy 92 a 95%. Również, jeśli chodzi o przyczyny naruszeń niezmiennie królują naruszenia związane z błędami w adresowaniu i wysyłce wiadomości elektronicznych.
Jedną z możliwych przyczyn tak znacznych dysproporcji w zakresie przyczyn naruszenia można upatrywać między innymi w tym, że działania umyślne mogą być trudniejsze do wykrycia niż niezamierzone, a więc statystycznie jest ich mało. Czytając raport pamiętajmy jednak, że naruszenia powstałe w wyniku działań nieumyślnych typu błędy w komunikacji mailowej zwykle dotyczą ograniczonej liczby odbiorców. W przypadku ataku hakerskiego (umyślność) skala dostępu do danych jest nieporównywalna i może w sumie być wyższa niż w przypadku 95% naruszeń wynikających z działań nieumyślnych. Dlatego przy analizowaniu nie wolno sugerować się jedynie udziałem procentowym przyczyn naruszeń i przy podejmowaniu działań mających przeciwdziałać ich wystąpieniu należy brać pod uwagę również skalę naruszenia. Na koniec warto też przypomnieć, że są incydenty „mieszane", gdzie nieumyślne nieprzestrzeganie stosowania procedur kończy się kradzieżą laptopa.

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 91,26% - przyczyny osobowe, 8,74% - przyczyny nieosobowe.

ZFODO mówi...

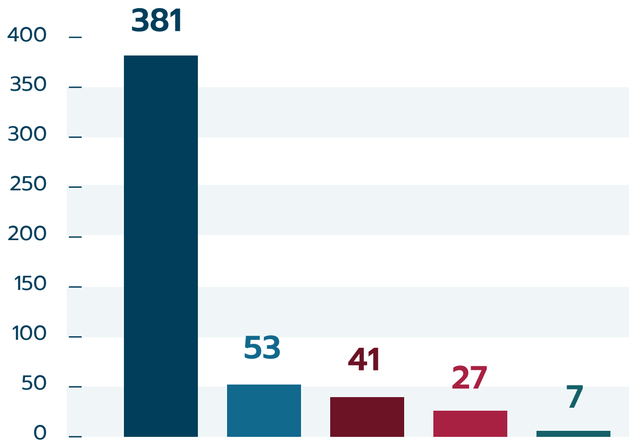
Michał Sztąberek
PREZES ZARZĄDU ISECURE SP. Z O.O

Szczerze powiedziawszy, w ogóle mnie nie dziwi, że dominują, i to już od paru lat (patrz: wcześniejsze raporty ZFODO dot. naruszeń), przyczyny osobowe jako źródło naruszeń ochrony danych osobowych. Z moich doświadczeń wynika, że zdecydowana większość incydentów to efekt mniejszego lub większego błędu pracownika lub współpracownika. A wiadomo, że o taki błąd jest bardzo łatwo. W iSecure, trochę przez łzy, śmiejemy się, że luty to miesiąc szczególny dla każdego IOD. Dlaczego? Otóż lada chwila będą wysyłane do pracowników i ex-pracowników druki PIT-11 i jak zawsze w tym okresie nastąpi wysyp naruszeń. Najczęściej będą one następstwem błędu człowieka odpowiedzialnego albo za wysyłkę, albo za aktualizowanie bazy danych kadrowych. I mimo, że PITy wysyłane są co roku, IOD stara się edukować, podejmowane są kolejne środki mające na celu minimalizację ryzyka wystąpienia incydentu, te jednak... stale się pojawiają. Być może problemem jest tu skala tego typu działań (a konkretnie wysyłki wielu dokumentów w tym samym czasie), ale przecież to nie powinno zwalniać pracowników odpowiedzialnych za ten proces od zachowania szczególnej ostrożności. W końcu mówimy tu o dość istotnych dla potencjalnego zainteresowanego danych osobowych.

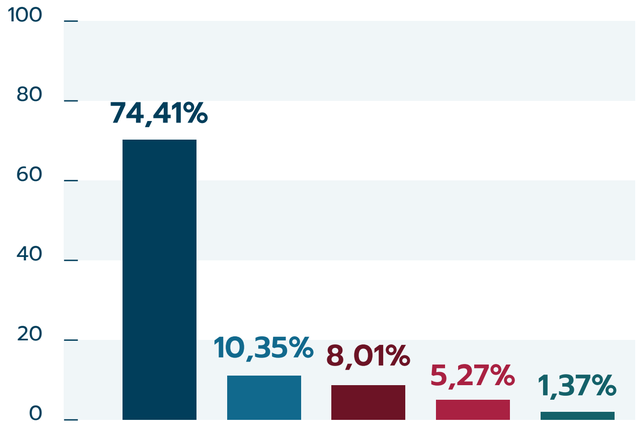
09

Najczęściej naruszane kategorie danych

Ile incydentów dotyczyło jednej z 5 kategorii danych:



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



- dane podstawowe
- PESEL
- Dane finansowe
- Dane szczególnej kategorii
- Dane dotyczące zachowań lub preferencji

- Wykres wskazuje na kategorie danych osobowych, których najczęściej dotyczy naruszenie. W tym roku zmieniliśmy sposób prezentowania kategorii naruszanych danych. Zdecydowaliśmy się pójść w kierunku systematyki ENISA. Więcej w komentarzu poniżej.

* Dane sumują się do więcej niż 100% ponieważ każdy z 250 incydentów mógł zawierać dane jednej lub większej ilosci kategorii

ZFODO mówi...

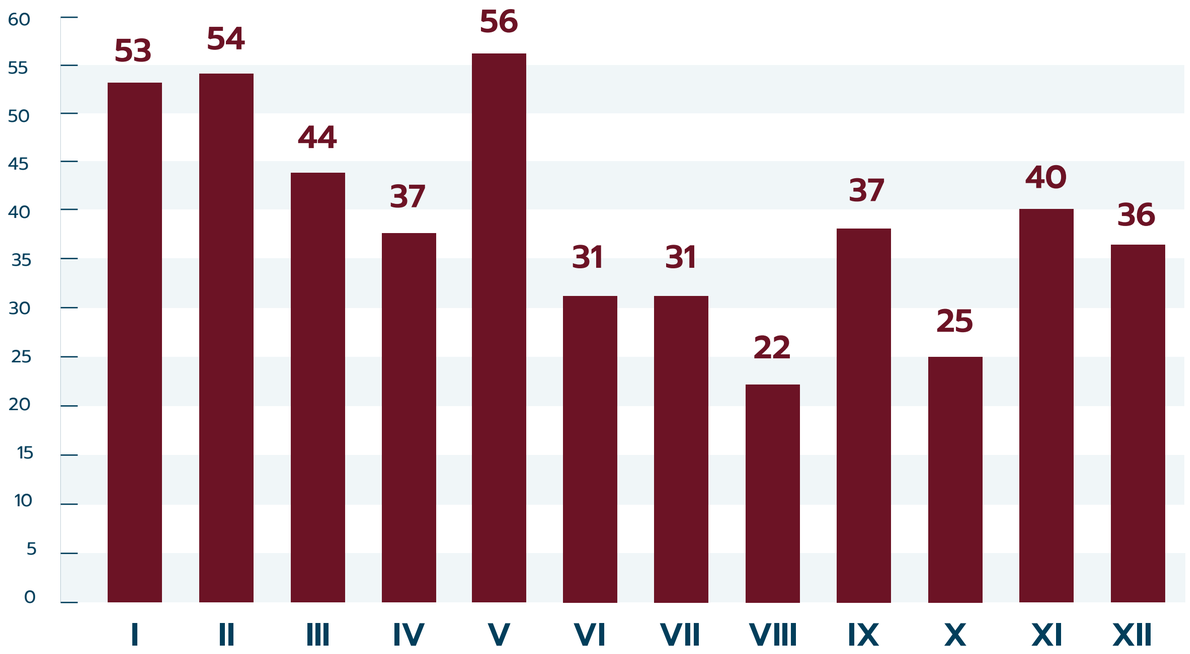
Michał Geilke

NSPEKTOR OCHRONY DANYCH/WŁAŚCICIEL ORLECCY-BEZPIECZEŃSTWO I EDUKACJA

Wykres wskazuje na kategorie danych osobowych, których najczęściej dotyczy naruszenie. W tym roku zmieniliśmy sposób prezentowania kategorii naruszanych danych. Zdecydowaliśmy się pójść w kierunku systematyki ENISA. Więcej w komentarzu poniżej.

Z innej części naszego raportu „Branże najbardziej narażone na ryzyko naruszeń ochrony danych osobowych" wynika, że branża handlowa i e-commerce miała najwięcej incydentów związanych z naruszeniem bezpieczeństwa danych– 35,9%.
Tym bardziej przedstawione statystyki nie powinny szczególnie dziwić, dane podstawowe jak np. imię i nazwisko i adres zamieszkania/do doręczeń osoby fizycznej jest najczęściej podawaną daną np. w usługach on-line jak sklepy internetowe.
Jednocześnie trudno sobie wyobrazić funkcjonowanie pozostałych branż jak finanse czy ubezpieczenia bez możliwości pozyskiwania i dalszego przetwarzania podstawowych danych osobowych beneficjentów tego typu usług.
Ilość miejsc, gdzie podmiot danych przekazuje swoje podstawowe dane osobowe jest dosłownie ogromna. To z kolei jest czynnikiem zwiększającym ryzyko wystąpienia niepożądanego zdarzenia odnoszącego się do tych danych.

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...

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.

11 Zawiadomienie organów ścigania

- W tym roku wprowadzamy nową statystykę, która dotyczy incydentów zgłoszonych organom ścigania. Blisko 7,74% naruszeń, została zgłoszona organom ścigania. To trzykrotnie mniej, niż liczba naruszeń, które trafiły do Organu Nadzorczego. W kolejnych będziemy mogli skomentować szerzej trendy w tej statystyce.

ZFODO mówi...

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

Naruszenia zaraportowane organom ścigania, to naruszenia o najpoważniejszych konsekwencjach. W ostatnim okresie raportowym, blisko 8% wszystkich naruszeń, zostało zgłoszonych organom ścigania. Wprowadziliśmy nową statystykę, będziemy obserwować trend!

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