ZFODO

Incydenty ochrony danych osobowych 2021

Raport Związku Firm Ochrony Danych Osobowych

00 O raporcie

- Badaniem objęliśmy **349 organizacji** obsługiwanych przez Firmy zrzeszone w ramach ZFODO w okresie **maj 2020 – maj 2021**.
- 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

309
odnotowanych incydentów

349
organizacji

0,89
średnia liczba incydentów przypadających na organizację

- Badaniem objęliśmy 349 organizacji, obsługiwanych przez 8 różnych firm zrzeszonych w ramach ZFODO w zakresie outsourcingu IOD lub innej stałej współpracy dotyczącej ochrony danych osobowych. Łącznie w okresie od 25 maja 2020, do 25 maja 2021, w ww. liczbie organizacji, odnotowano 309 incydentów.

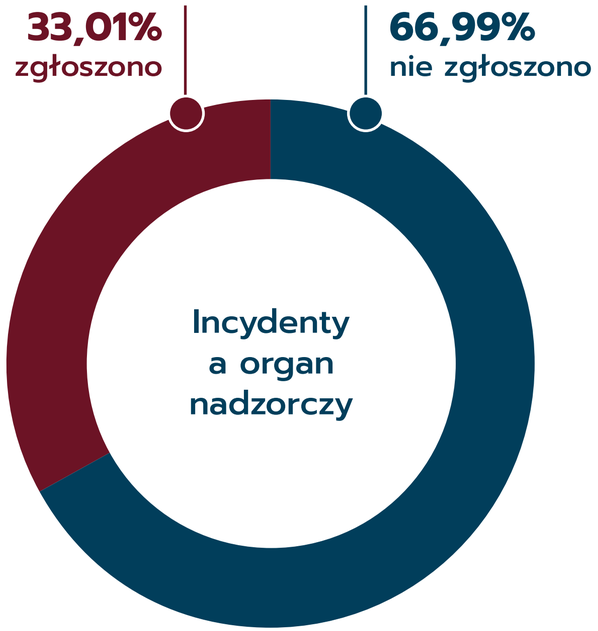
Daje to średnią 0,89 incydentu rocznie na każdą organizację. Badanie opieramy na incydentach, które zostały zgłoszone firmom zrzeszonym w ZFODO przez obsługiwane przez nich organizacje. Liczba incydentów, które wystąpiły w rzeczywistości może być wyższa.

ZFODO mówi...

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

Średnia ilość incydentów przypadających na organizacje zbliża się do jednego incydentu rocznie. Wszystko wskazuje na to, że ta średnia będzie dalej rosła. Czy to znaczy, że RODO i systemy ochrony danych osobowych są coraz mniej skuteczne? Taki wniosek nie będzie w mojej opinii trafny, chociaż może być pierwszym, który się nasuwa, po analizie statystyk. Trzeba wziąć pod uwagę przede wszystkim dwa dodatkowe czynniki. Po pierwsze wciąż rośnie wykrywalność incydentów i świadomość organizacji. Sytuacje, które kiedyś w ogóle nie były traktowane jako incydenty, dzisiaj już są. Po drugie, wciąż rośnie skala przetwarzania danych osobowych. Im więcej operacji na danych, tym większa szansa zaistnienia incydentu.

03 Incydenty zgłoszone organowi nadzorczemu



- Blisko 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.”*

Daje to średnią 0,89 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.

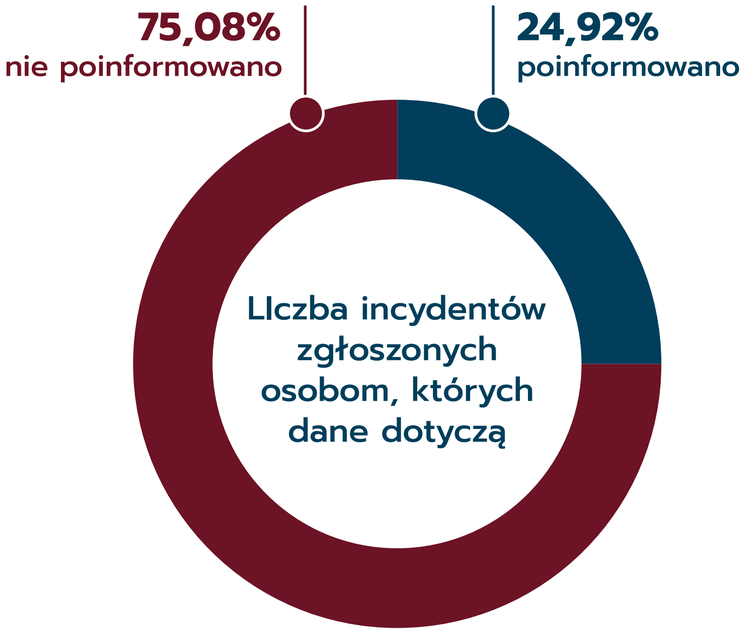
ZFODO mówi...

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

Szczerze powiedziawszy, jestem nieco zaskoczony tym, że choć znamy podejście UODO do incydentów, gdzie pojawia się nr PESEL (z poczynionych obserwacji wynika, że Regulator oczekuje w takim przypadku zgłoszenia) w zasadzie statystki dotyczące notyfikacji naruszeń nie zmieniły się niemal w ogóle w stosunku do tego co odnotowaliśmy w roku ubiegłym (dla przypomnienia - wówczas 66,99% incydentów nie zostało przekazanych do analizy do Regulatora, obecnie to 67%, czyli - jak widać – różnica jest na poziomie błędu statystycznego). Wydawać by się mogło, że mając taką wiedzę, administratorzy będą zgłaszać naruszenia na potęgę, a okazuje się, że nic w tym zakresie w zasadzie się nie zmieniło. Może to i dobrze, bo - i piszę to z praktycznego punktu widzenia - często, gdy analizujemy incydent metodą ENISA i to właśnie taki, gdzie pojawia się PESEL np. źle przesłany roczny PIT - wychodzi, że ryzyko naruszenia praw i wolności jest niskie. Ot, taka sprzeczność - uznawana metoda oceny incydentów vs. praktyka przed Regulatorem. A może patrzę na to zbyt pesymistycznie? Może po prostu okrzepliśmy już z naruszeniami i wiemy co zgłaszać do UODO, a co wystarczy wpisać do stosownego rejestru (oczywiście wraz z podjęciem stosownych działań naprawczych, by zminimalizować wystąpienie incydentu w przyszłości).

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 70% przypadków.

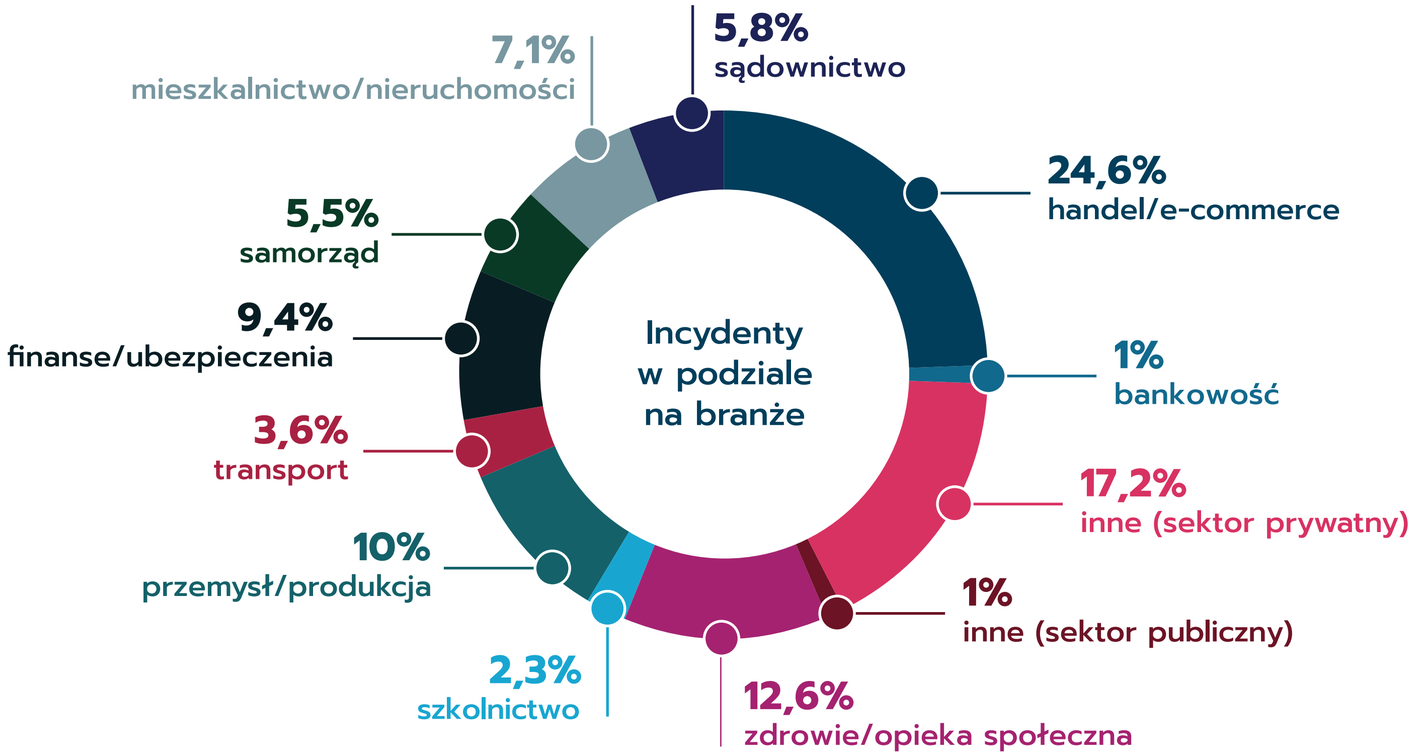
ZFODO mówi...

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

Biorąc pod uwagę dane z poprzedniego raportu ZFODO „Incydenty ochrony danych osobowych maj 2019-maj 2020" oraz obecny raport za okres od maja 2020 do maja 2021 widać wyraźną tendencję wzrostową średniej ilość incydentów przypadających na organizację, pomimo mniejszego udziału całkowitej liczby organizacji w obecnym raporcie (obecnie 349 administratorów, poprzednio 454 administratorów). Blisko 25% wskaźnik incydentów zgłoszonych osobom, których dane dotyczą w związku z prawdopodobieństwem wystąpienia ryzyka naruszenia praw lub wolności tych osób w zestawieniu z ponad 75% ilością niezgłoszonych naruszeń, wskazywać może na dużo większą świadomość w postępowaniu z naruszeniami ochrony danych osobowych. Po trzyletnim stosowaniu rozporządzenia RODO duży wpływ na informowanie lub brak poinformowania osoby, której dane dotyczą ma niewątpliwie doświadczenie administratora związane ze sposobem analizy incydentu również w kontekście dostępnego orzecznictwa i opinii organu nadzorczego. Na uwagę zasługuje również fakt, że w tym czasie nie tylko administrator zdobył kompetencje co do postępowania z naruszeniami, ale także pracownicy (podmioty danych) mają większą świadomość ochrony danych osobowych i realizacji swoich praw wynikających z RODO.

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 35%).

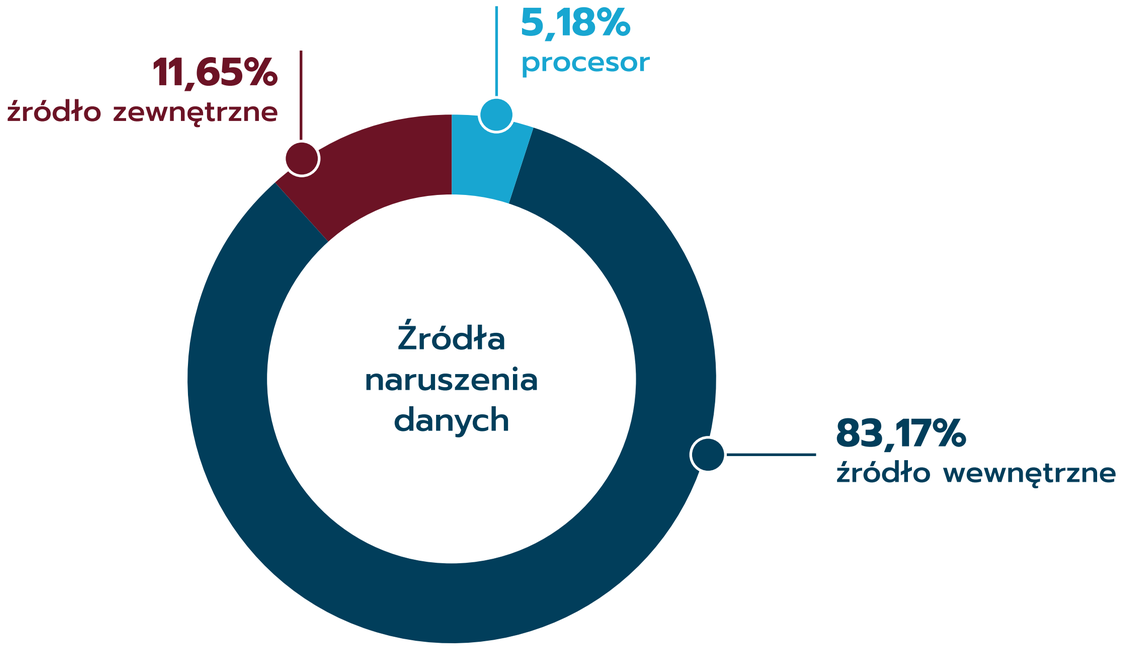
ZFODO mówi...

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

Bardzo ciekawie prezentują się dane statystyczne dotyczące branż, w których wystąpiło najwięcej incydentów. W poprzednim roku taką branżą był bliżej niesklasyfikowany sektor prywatny, obecnie zaś "liderem" jest handel / e-commerce. Wydaje mi się, że wpływ na to mogła mieć pandemia i dużo większa sprzedaż on-line. Sprzedaż była często prowadzona przez firmy, które do tej pory nie miały swoich sklepów internetowych. Przedłużający się okres obostrzeń związanych z COVID-19, zamknięte całe branże - to wszystko sprawiło, że wiele przedsiębiorstw do tej pory sprzedających tylko off-line, weszło w segment on-line, a to mogło wiązać się z problemami wieku dziecięcego, czyli choćby nieco mniejszym doświadczeniem przy obsłudze zamówień internetowych i wynikających z tego pomyłek np. błędnie przesłane zamówienie / faktura i incydent gotowy.

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.

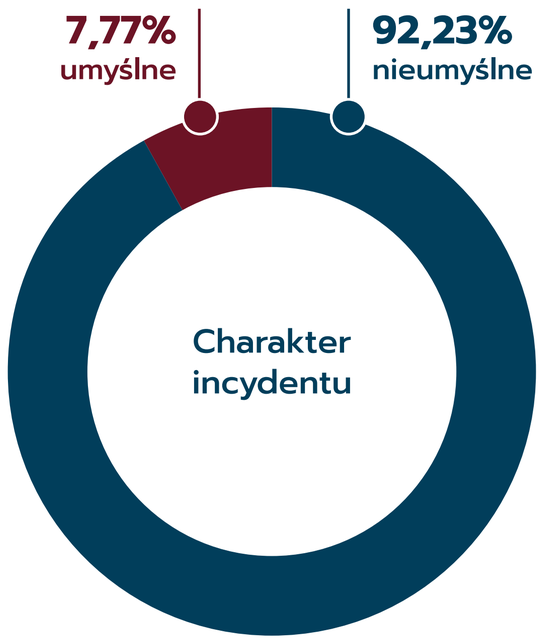
ZFODO mówi...

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

Administratorzy danych nie do końca posiadają wpływ na działania hakerów, byłych pracowników, czy innych podmiotów nie działających w dobrej wierze. Statystyka pokazuje jednak, że są dość dobrze przygotowani na działanie czynników zewnętrznych prowadzących do naruszeń. Jeszcze lepiej administratorzy zabezpieczyli swoje relacje z podmiotami przetwarzającymi, bowiem procesorzy odpowiadają wyłącznie za 5,18% wszystkich naruszeń. Jednocześnie, większość przyczyn naruszeń tkwi niezmiennie wewnątrz organizacji. To cenna wskazówka zarówno dla administratorów, podmiotów przetwarzających oraz Inspektorów Ochrony Danych, aby znaczną część działań audytowych i szkoleniowych kierować do swoich pracowników i współpracowników.
Z pewnością warto raz jeszcze przeprowadzić analizę własnych rejestrów naruszeń oraz sposobów działania ze stwierdzonymi lub potencjalnymi naruszeniami. Trzymam kciuki za wszystkich Inspektorów Ochrony Danych, którym uda się całkowicie zapobiec lub ograniczyć powtarzalność naruszeń stwierdzonych w przeszłości!

07

Umyślność bądź nieumyślność incydentu



- **Aż 92% incydentów stanowiły działania nieumyślne (w poprzednim badaniu statystyka wyglądała podobnie). 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 Geilke

INSPEKTOR OCHRONY DANYCH/WŁAŚCICIEL ORLECCY-BEZPIECZEŃSTWO I EDUKACJA

„Nie myli się tylko ten, kto nic nie robi.” To powiedzenie pasuje idealnie do procentowego wyniku analizy incydentów związanych z przetwarzaniem danych osobowych pod kątem ich umyślności/nieumyślności.
Statystyka w porównaniu do poprzedniego raportu jest niemal identyczna i wskazuje, że jeśli coś w danym podmiocie już się wydarzy (w rozumieniu incydentu) to będzie to zdarzenie spowodowane działaniem nieumyślnym.
Ponownie, większość zdarzeń nieumyślnych jest powiązana z pracą, z korespondencją elektroniczną. Zdarzenia te mają różne charakterystyki, jak np. błędnie adresowana korespondencja (przykładowo spowodowana podobną konstrukcją samego adresu e-mail) czy przesyłanie niewłaściwych załączników (chodzi zarówno o zdarzenia, gdzie cały załącznik nie powinien trafić do danej osoby jak i jego część, np. plik formatu Excel z o jednym za dużo arkuszem).
Warto tutaj wspomnieć również o zdarzeniach umyślnych związanych z obsługą i zabezpieczaniem korespondencji elektronicznej jak np. celowe nieszyfrowanie załączników, bo klient prosił, bo klientowi to utrudnia „życie” itp.
Niestety, przeciwdziałanie tego typu sytuacjom bez dedykowanych systemów informatycznych lub rozwiązań w nich implementowanych (przykładowo można podać opóźnienie czasowe faktycznej wysyłki wiadomości, którą posiada np. system Gmail) jest bardzo trudne.

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 95,95% - przyczyny osobowe, 4,05% - przyczyny nieosobowe.

ZFODO mówi...

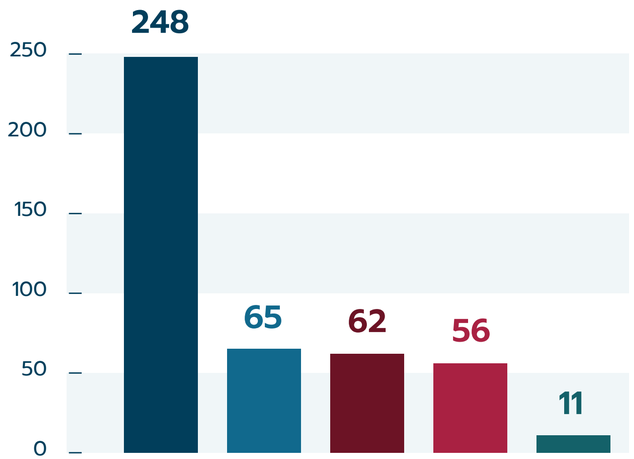
Tomasz Osiej
PREZES ZARZĄDU OMNI MODO SP. Z O.O.

Porównując dane rok do roku widać wyraźny (z 4,05% do 8,41%.) wzrost przyczyn nieosobowych w ogólnej statystyce naruszeń. Wzrost ten sugeruje, wręcz woła o większą uwagę co do konieczności wykonywania privacy by design, privacy by default czy analiz ryzyka wykorzystywanych narzędzi.
Przyczyny na styku technologii i osób są nową kategorią, ale można spodziewać się, że jej znaczenie może wzrosnąć w kolejnych latach w związku z rozwojem takich technologii jak sztuczna inteligencja.
Prowadzi to wprost do wniosków, że procedury ochrony danych osobowych powinny nie tylko być przyjęte w organizacji, ale przede wszystkim być realnie stosowane. Dopiero ich właściwe wdrożenie będzie można nazywać sukcesem.
Nieustanie powinniśmy uświadamiać i przypominać wszystkim w organizacji jak ważna jest ochrona danych osobowych i że jest to zadaniem każdego z nas i w każdym czasie. Ochrona danych to projekt korporacyjny. Przetwarzajmy i chrońmy dane osobowe jakby to były nasze własne dane osobowe.

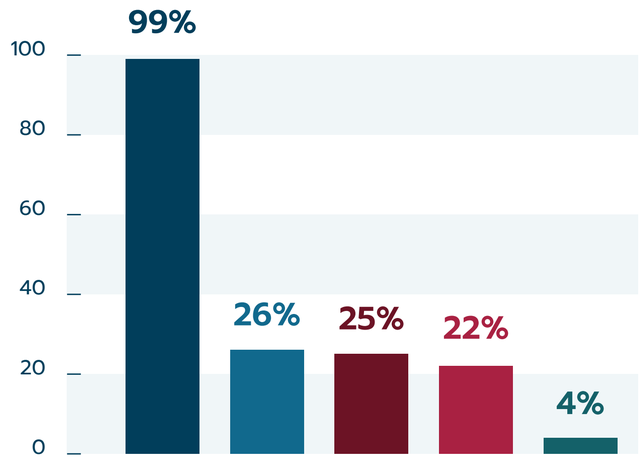
09

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.

* Ta statystyka odnosi się łącznie do 250 incydentów

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

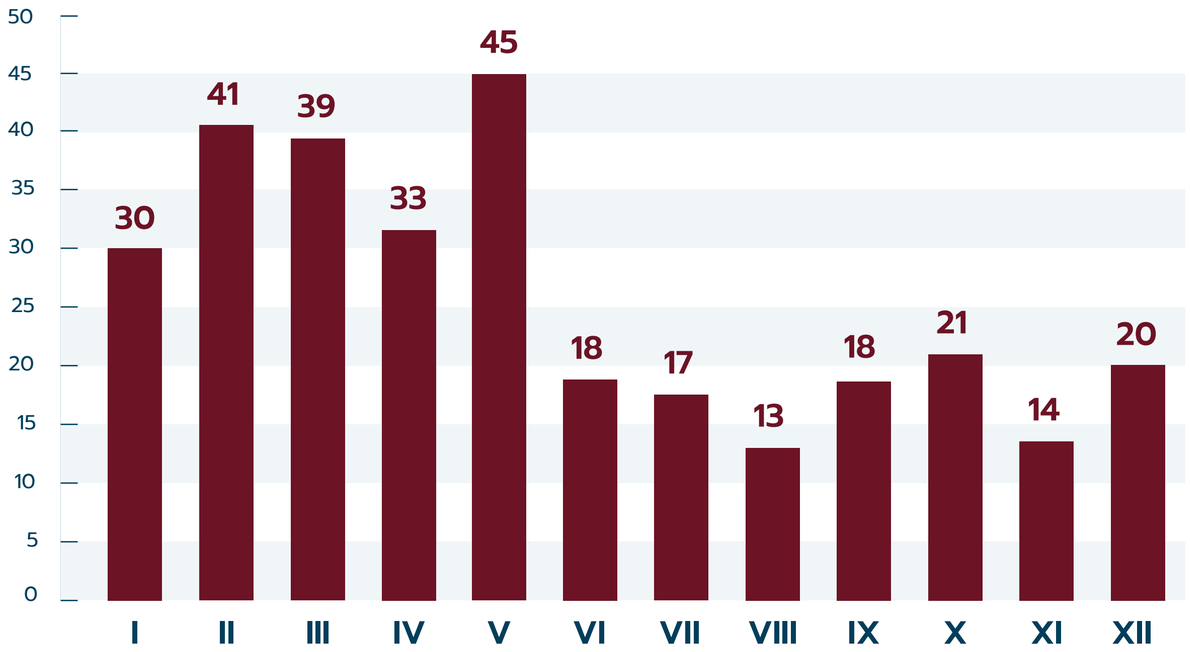
ZFODO mówi...

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

Podział na kategorie danych jest zgodny z podziałem dokonanym przez European Union Agency for Network and Information Security (ENISA): dane podstawowe, behawioralne, finansowe i dane szczególnych kategorii, potocznie zwane również danymi wrażliwymi.

Dodatkowo wyodrębniliśmy zbiór, w przypadku którego naruszeniu uległ również nr PESEL. Nasze badanie pokazuje, że o ile praktycznie zawsze naruszeniu bezpieczeństwa podlegają dane podstawowe, to zaskakująco często naruszenie dotyczy danych finansowych (tajemnica przedsiębiorstwa), danych szczególnych kategorii (bardzo prywatnych), jak i numeru PESEL, co powinno skutkować powiadomieniem Prezesa UODO oraz osób, których dane dotyczą. Proszę mieć na uwadze, że w jednym incydencie mogła pojawić się jedna kategoria danych, dwie, lub nawet wszystkie pięć, stąd procenty nie sumują się do 100%.

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...

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

W zakresie miesięcy obfitujących w naruszenia wciąż trudno o wskazanie jednoznacznych trendów. Wyraźnie widać spadek incydentów w okresie wakacyjnym, co jest łatwe do wytłumaczenia. Z drugiej strony końcówka roku, która najczęściej jest bardzo intensywna w większości branż, nie obfituje w incydenty, tak jak początek roku. W przyszłym roku zestawimy dane ze wszystkich lat od początku prowadzenia statystyk i poszukamy prawidłowości w długofalowych statystykach.

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