

RAPORT 2015



CO WIEMY O OCHRONIE
DANYCH OSOBOWYCH

ODO24.pl

› *Spis treści:*

› Elektronika – nasza codzienność!	4
Najpopularniejsze urządzenia elektroniczne.....	5
› Jak dbamy o swoje dane?	6
Ryzyko nieodwracalnej utraty danych.....	7
Kopiowanie danych	7
Kradzież danych.....	8
Największe zagrożenia dla danych osobowych	8
› Naruszenia prawa do ochrony swoich danych osobowych	9
Naruszenia prawa do prywatności.....	10
Sposoby wykorzystania bezprawnie pozyskanych danych	11
› Przetwarzanie danych osobowych w firmach i instytucjach	12
Szkolenia	13
Wiedza.....	13
Incydenty.....	13
› Administrator bezpieczeństwa informacji (ABI)	15
ABI w organizacji	16
› Opinie na temat nowelizacji ustawy o ochronie danych osobowych ze stycznia 2015 r.	17
› Charakterystyka respondentów	19



ODO 24 sp. z o.o. specjalizuje się w ochronie danych osobowych dostarczając nowoczesne, elastyczne i kompleksowe rozwiązania, pomagające zapewnić zgodność z ustawą o ochronie danych osobowych. Na ofertę ODO 24 składają się m. in.: outsourcing funkcji administratora bezpieczeństwa informacji (ABI), wsparcie ABI, szkolenia administratorów i pracowników, bezpłatne porady prawne oraz opiniowanie umów z zakresu ochrony danych osobowych. Poprzez swoją stronę internetową firma bezpłatnie udostępnia Biuletyn informacyjny, oraz aplikację ABLeve, wspierającą sprawne zarządzanie systemem ochrony danych osobowych w każdej organizacji.

ODO 24 kompleksowo dostosowuje podmioty do wymogów prawa, ze szczególnym uwzględnieniem bezpieczeństwa przetwarzanych przez nie danych. Swoją działalność dedykuje wszystkim tym, którzy chcą poznać, zrozumieć i wdrożyć zasady ochrony danych osobowych.

Raport

Powstał na podstawie badania przeprowadzonego w dniach 01.07.2015 – 15.08.2015 r. na grupie 1 076 internautów. Narzędziem badawczym była ankieta online, zamieszczona na stronie internetowej ODO24.pl

Autorzy

Maciej Kaczmarek, Leszek Kępa, Tomasz Ochocki, Maciej Jurczyk, Dominik Kantorowicz

Ilustracje

Karol Banach (karolbanach.com)

Projekt i skład

Radek Zgódka (radekzgodka.pl)

Redakcja

Małgorzata Korólczyk-Rabek (gkrconsulting.pl)

ISBN: 978-83-943435-07

Warszawa, grudzień 2015 r.

Wszelkie prawa zastrzeżone.

Zarówno publikacja w całości jak też każdy jej fragment nie mogą być powielane ani rozpowszechniane w żadnej formie i w żaden sposób bez uprzedniego pisemnego zezwolenia ODO 24 sp. z o.o. Wszelkie znaki towarowe, znaki graficzne, nazwy własne, logotypy i inne dane są chronione prawem autorskim i należą do ODO 24 sp. z o.o.

› Słowo wstępu

Oddajemy w Państwa ręce pierwszy raport dotyczący badania społecznej świadomości tematyki ochrony danych osobowych i bezpieczeństwa informacji. Badanie przeprowadzone zostało na reprezentatywnej grupie 1 076 osób, a respondenci zostali podzieleni na 4 grupy ze względu na ich sytuację zawodową – osoby nieaktywne zawodowo, osoby zajmujące się przetwarzaniem danych w ramach swoich obowiązków służbowych, management lub właściciele oraz osoby pełniące funkcję ABl.

Co ciekawe, z raportu wynika, że świadomość zagadnień związanych z ochroną danych osobowych, nie jest w polskim społeczeństwie tak mała, jak mogłoby się w pierwszej chwili wydawać. Zaznaczyć jednak trzeba, że badanie zostało przeprowadzone wśród internautów, którzy ze względu na to, że na co dzień wykorzystują nowoczesne technologie, zazwyczaj wiedzą o nich i związanych z nimi zagrożeniach, nieco więcej.

Z raportu dowiedzą się Państwo m.in., że niemal 60% osób, których prywatność i prawo do ochrony danych zostały naruszone, nigdzie tego faktu nie zgłosiło, 42% spośród osób zarządzających firmami lub prowadzących własną działalność gospodarczą zupełnie nie obawia się ryzyka nieodwracalnej utraty przetwarzanych danych, a nielegalnie pozyskane dane są najczęściej wykorzystywane w celach marketingowych. Każdy dział raportu kończy się komentarzem naszego eksperta, który krótko podsumowuje i analizuje przedstawione wyniki.



Zachęcam do lektury

A stylized, handwritten signature in blue ink, appearing to read 'Maciej Kaczmarek'.

Maciej Kaczmarek
Prezes zarządu ODO 24 sp. z o.o.

Elektronika – nasza codzienność!



Laptopy są używane
dwa razy częściej niż komputery
stacjonarne, częściej nawet
niż smartfony.

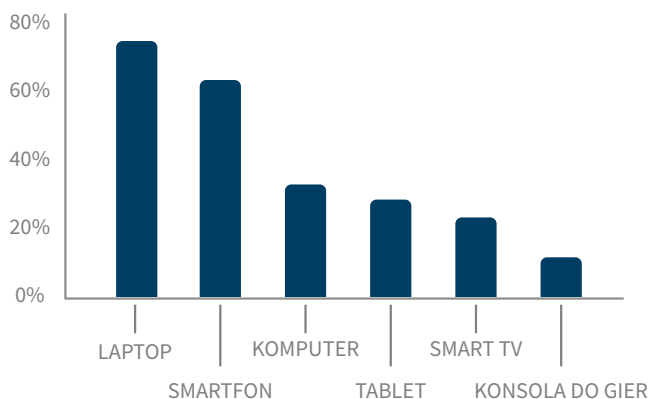
Współcześnie trudno już sobie nawet wyobrazić życie bez laptopów, smartfonów i innych elektronicznych udogodnień. Każdego roku producenci wprowadzają na rynek coraz ciekawsze i nowocześniejsze rozwiązania, dzięki którym zwykły, wydawałoby się, telefon czy tablet śmiało mogą już pełnić wszystkie funkcje małego biura.

› Najpopularniejsze urządzenia elektroniczne

Jak wynika z naszego badania, zdecydowanie najpopularniejszymi obecnie urządzeniami elektronicznymi są **laptopy i smartfony**.

Spośród 1072 ankietowanych, codziennie korzysta z nich odpowiednio 77% (laptopy) i 68% (smartfony) osób. Na kolejnych miejscach znalazły się komputery stacjonarne, tablety oraz telewizory typu smart, dekodery oraz konsole do gier z dostępem do internetu. W badaniu można było wskazać więcej niż jedno urządzenie.

KORZYSTANIE Z URZĄDZEŃ ELEKTRONICZNYCH

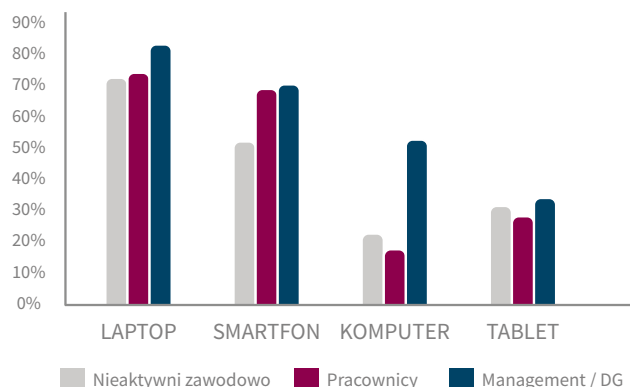


Powyższy wykres przedstawia procentowy rozkład wyników dla poszczególnych urządzeń elektronicznych.

Zarówno osoby nieaktywne zawodowo (studenci, bezrobotni), jak też pracujący **korzystają głównie ze smartfonów i laptopów**.

Uwagę zwraca jednak wysoki odsetek wskazań wykorzystywania komputerów stacjonarnych przez **kadry zarządzające i osoby prowadzące działalność gospodarczą**. W tej grupie respondentów jest to aż 56%, podczas gdy w innych grupach odsetek ten wyniósł 23% (nieaktywni zawodowo) i 19% (pracownicy).

RÓŻNICE W WYKORZYSTYWANIU URZĄDZEŃ ELEKTRONICZNYCH



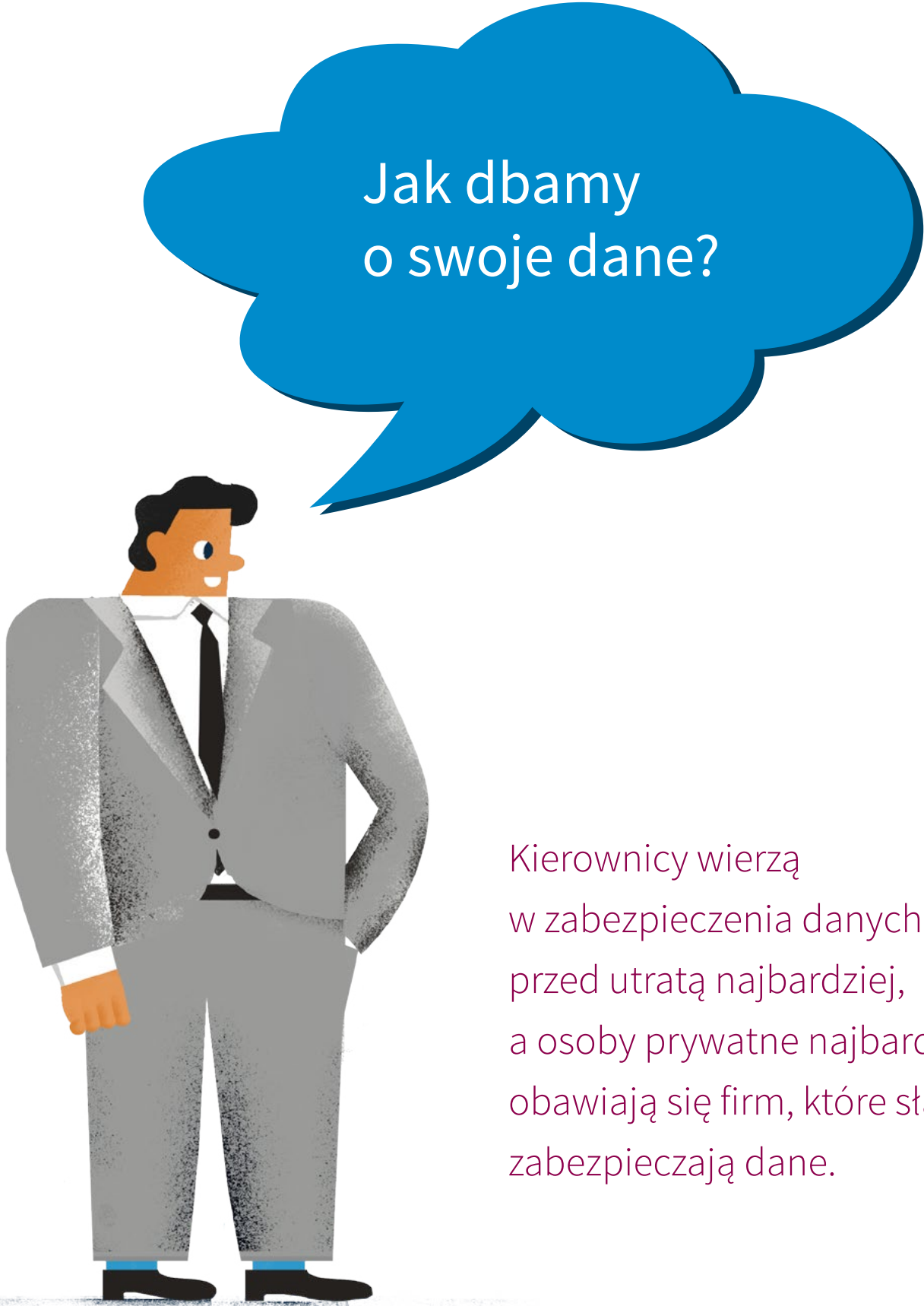
Różnicę widać również w przypadku korzystania ze smartfonów. **Wśród nieaktywnych zawodowo korzysta z nich 53% osób**, podczas gdy w pozostałych grupach 71% (management) i 70% (pracownicy).

Dzielimy się wiedzą

[ODO24.pl/blog](https://odo24.pl/blog)

OKIEM EKSPERTA

Biorąc pod uwagę fakt, że współcześnie przetwarzanie danych nierozdzielnie łączy się z wykorzystywaniem nowoczesnych technologii, wyniki badania zdecydowanie nie dziwią. Warto jednak pamiętać, że do określonego rodzaju sprzętu należy stosować odpowiednie środki techniczne i organizacyjne, zapewniające ochronę przetwarzanych danych osobowych. Ochrona ta powinna być adekwatna do zagrożeń oraz kategorii danych objętych ochroną. W szczególności należy właściwie zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym (art. 36.1 ustawy o ochronie danych osobowych). Zalecamy więc stosowanie chociażby podstawowych zabezpieczeń, takich jak szyfrowanie pamięci, autoryzacja dostępu oraz kontrola wysyłanych treści.

A stylized illustration of a man with orange skin, wearing a grey suit, white shirt, and black tie. He is standing with his hands on his hips. Above him is a large blue thought bubble containing the text 'Jak dbamy o swoje dane?'.

Jak dbamy
o swoje dane?

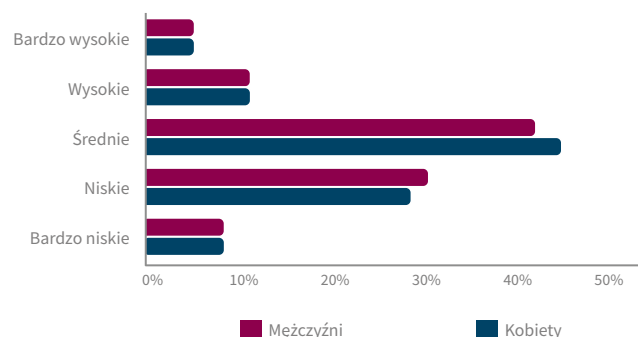
Kierownicy wierzą
w zabezpieczenia danych
przed utratą najbardziej,
a osoby prywatne najbardziej
obawiają się firm, które słabo
zabezpieczają dane.

Współcześnie informacja to potęga. Kto ma dostęp do danych i potrafi nimi odpowiednio zarządzać – wygrywa. Dotyczy to także, a może nawet przede wszystkim, danych osobowych. Dla różnego rodzaju firm i instytucji odpowiednio opracowane bazy danych są niejednokrotnie na wagę złota. Czy jednak, w związku z tym, przykładamy odpowiednią wagę do zapewnienia danym bezpieczeństwa – zarówno swoim własnym, jak też powierzonym zbiorom?

› Ryzyko nieodwracalnej utraty danych

Z przeprowadzonego badania wynika, że zdecydowana **większość respondentów w niewielkim stopniu obawia się nieodwracalnej utraty danych**. 45% z nich takie ryzyko określiło jako średnie, a 30% – jako niskie. Nieco bardziej ostrożne wydają się być kobiety – niskie ryzyko zaznaczyło 29%, podczas gdy w przypadku mężczyzn było to 31%. Wielkości wskazań pozostałych odpowiedzi w obu grupach były bardzo porównywalne.

OCENA RYZYKA NIEODWRACALNEJ UTRATY DANYCH WŚRÓD KOBIET I MĘŻCZYŹN

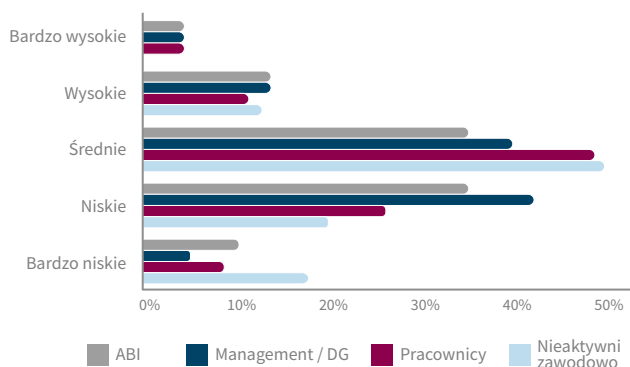


Dużo większe zróżnicowanie w odpowiedziach uzyskaliśmy przy porównaniu poszczególnych grup respondentów. Okazało się, że **większość przedstawicieli managementu** ryzyko nieodwracalnej utraty danych w swoich organizacjach **uznała za niskie** – taką odpowiedź wskazało 42% respondentów. Wśród takiej oceny ryzyka, odpowiedzi kierownictwa było zdecydowanie najwięcej. Wśród **administratorów bezpieczeństwa informacji**, ryzyko jako **niskie** określiło 35% osób, niemal identycznie jak wśród wskazań dla **średniego stopnia** ryzyka.

Warto zwrócić uwagę na rozkład odpowiedzi, określających ryzyko utraty danych jako **bardzo niskie**. Najwięcej takich odpowiedzi wskazały **osoby nieaktywne zawodowo** – 17%. W pozostałych grupach,

odpowiedzi te stanowiły kolejno 10% (ABI), 8% (pracownicy) i 5% (management).

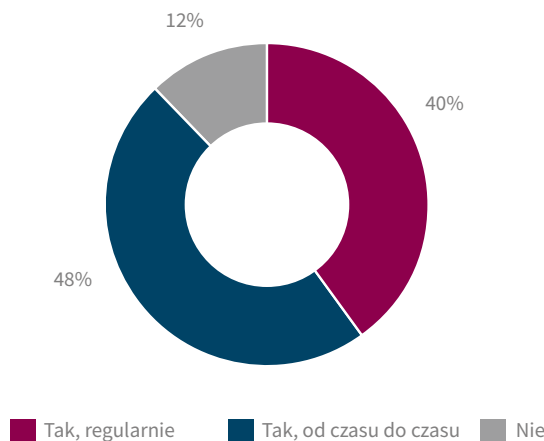
OCENA RYZYKA NIEODWRACALNEJ UTRATY DANYCH W PODZIALE NA GRUPY



› Kopiowanie danych

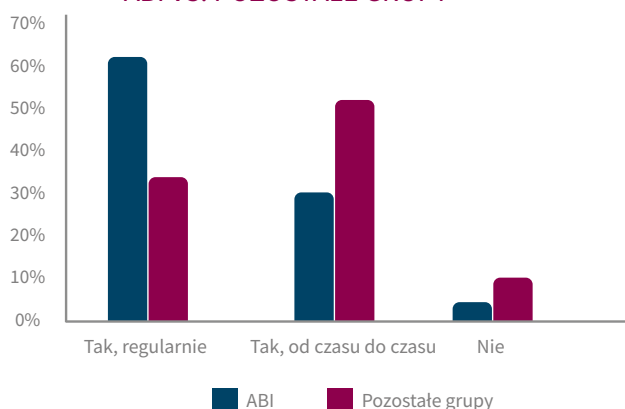
Mimo że większość osób określa ryzyko nieodwracalnej utraty danych jako co najwyżej średnie, to jednak aż **88% respondentów robi kopie swoich danych, a 40% robi to regularnie**.

CZY WYKONUJESZ KOPIE SWOICH DANYCH?



Ciekawie wygląda przy tym porównanie pomiędzy osobami pełniącymi funkcję administratorów bezpieczeństwa informacji a przedstawicielami pozostałych badanych grup. **62% ABI regularnie wykonuje kopie swoich danych**. Nie wykonuje ich zaledwie 6%. Wśród pozostałych respondentów, regularne wykonywanie kopii zadeklarowało 35%, a nie wykonywanie ich wcale – 12%.

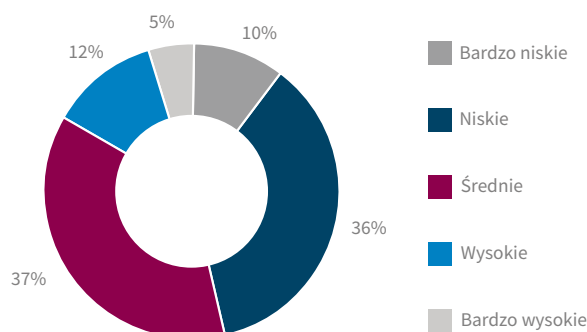
CZY WYKONUJESZ KOPIE SWOICH DANYCH? ABI VS. POZOSTAŁE GRUPY



› Kradzież danych

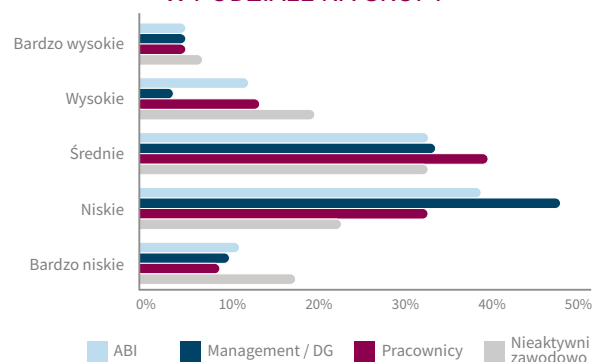
Respondentów zapytaliśmy również o ocenę ryzyka kradzieży danych. Podobnie jak w pytaniu o ryzyko utraty danych, tutaj też przeważały **odpowiedzi o ryzyku średnim (37%) i niskim (36%)**. Szczegółowy rozkład odpowiedzi na poniższym wykresie.

OCENA RYZYKA KRADZIEŻY DANYCH OSOBOWYCH



Porównaliśmy też odpowiedzi poszczególnych grup. I tu również bardzo niskie ryzyko kradzieży danych zaznaczyła większość osób nieaktywnych zawodowo (17%), a niskie – kadra zarządzająca (47%). **Odpowiedzi większości ABI-ch znajdują się we wskazaniach ryzyka niskiego (39%) i średniego (33%).**

OCENA RYZYKA KRADZIEŻY DANYCH OSOBOWYCH W PODZIALE NA GRUPY



› Największe zagrożenia dla danych osobowych.

Wśród największych zagrożeń dla bezpieczeństwa danych osobowych respondenci zdecydowanie najczęściej wskazywali **firmy i organizacje nieprzysięgające wagi do ochrony przetwarzanych danych osobowych (32%)**, **przestępczość internetową (31%)** oraz różnego rodzaju **organizacje, które z chęci zysku wykorzystują dane bez zgody osób, których dotyczą (27%)**. Zdecydowanie niżej w rankingu znalazły się oszczędności firm kosztem właściwej ochrony danych oraz niewystarczająca wiedza nas samych lub też naszych znajomych czy współpracowników. Co warto zaznaczyć, zaledwie dwie osoby nie dostrzegły w swoim otoczeniu żadnych zagrożeń dla bezpieczeństwa danych.

NAJWIĘKSZE ZAGROŻENIA DLA DANYCH



OKIEM EKSPERTA

Nowoczesne technologie to, z jednej strony, ogromne ułatwienie i wygoda szybkiego dostępu do danych, z drugiej, niestety, znaczny wzrost ryzyka utraty danych lub ich niezamierzonego udostępnienia – uszkodzenie nośnika, kradzież czy włamanie. Okazuje się jednak, że ryzyko tych zagrożeń jest często bagatelizowane – wydaje nam się, że prawdopodobieństwo ich wystąpienia jest znikome.

To sytuacja całkowicie niezrozumiała. Sprzęt elektroniczny, którym się współcześnie posługujemy bywa, wbrew zapewnieniom ich producentów, zawodny i podatny na uszkodzenia, a korzystanie z WiFi czy Bluetooth, umożliwia podsłuchanie transmisji danych. Warto więc uniemożliwić nieautoryzowany dostęp do urządzeń (np. oddając sprzęt do serwisu) i właściwie zabezpieczyć znajdujące się na nich dane.

Naruszenia prawa do ochrony swoich danych osobowych



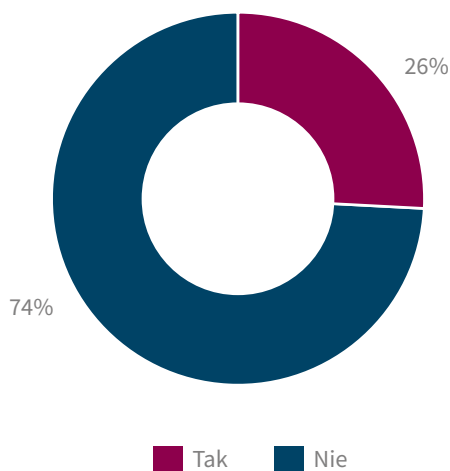
Ankietowani nie zgłaszają
incydentów bo nie wierzą
w skuteczność postępowania.

To, czy nasze dane będą bezpieczne zależy w dużej mierze od nas samych. Jeśli sami nie będziemy zwracać właściwej uwagi na ochronę swojej prywatności, trudno liczyć na to, że zapewnią to nam jakiekolwiek przepisy prawa czy polityki bezpieczeństwa. Dotyczy to zarówno działań prewencyjnych, jak też tych, które powinniśmy podjąć, gdy ktoś bezprawnie wykorzysta nasze dane. A jak to wygląda w praktyce?

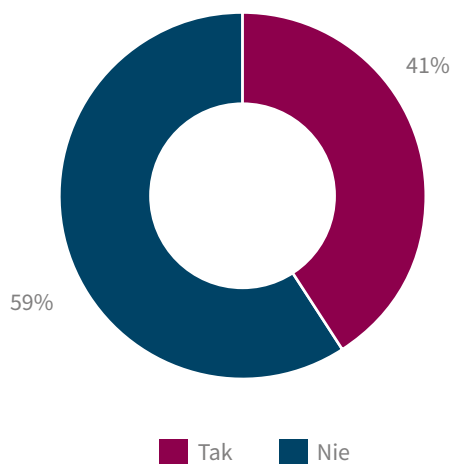
› *Naruszenia prawa do prywatności*

Zapytaliśmy respondentów o to, czy kiedykolwiek naruszono ich prawo do prywatności – wykradziono ich dane osobowe, wykorzystano dobrowolnie przekazane dane w innym celu niż ten, dla którego były gromadzone, udostępniono dane osobom nieuprawnionym, itp. Okazało się, że **zaledwie 26% respondentów spotkało się z naruszeniem ich prawa do ochrony danych osobowych**.

CZY KIEDYKOLWIEK NARUSZONO TWOJE PRAWO DO OCHRONY DANYCH OSOBOWYCH?



CZY ZGŁOSIŁEŚ TEN INCYDENT?



BEZPŁATNY PRAKTYCZNY PORADNIK

“Jak w praktyce i zgodnie z prawem przetwarzać dane osobowe”.

Uwzględnia nowelizację ustawy i rozporządzenia

GRATIS

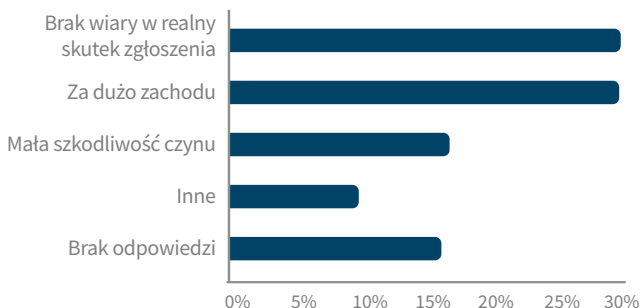


SPRAWDŹ

Co więcej, w zdecydowanej większości przypadków, incydenty te nie zostały nigdzie zgłoszone. Niemal 60% ankietowanych przyznało, że nie zrobiło niczego, by ukarać czy choćby upomnieć winnych.

Na pytanie o powody niezgłoszenia naruszenia swojego prawa do prywatności respondenci niemal na równi wskazali **brak wiary w realny skutek takiego zgłoszenia** oraz obawę o **zbyt dużą ilość** związanych z tym **formalności i stratę czasu** – „za dużo zachodu”. Obie odpowiedzi uzyskały po 29% wskazań. Kolejne miejsce zajęło przekonanie o małej szkodliwości incydentu. Co ciekawe, aż 16% ankietowanych nie udzieliło odpowiedzi na to pytanie.

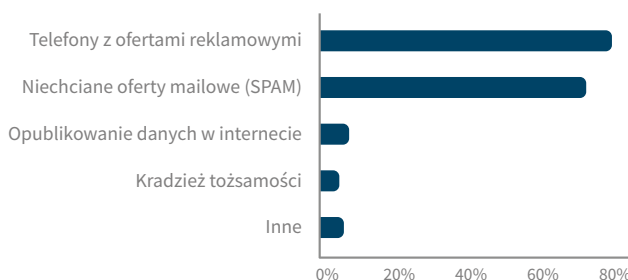
POWODY NIEZGŁOSZENIA INCYDENTU



› Sposoby wykorzystania bezprawnie pozyskanych danych

Zdecydowanie najczęściej wskazywanymi sposobami wykorzystania danych są **telefony z ofertami reklamowymi** oraz rozsyłany mailowo **SPAM**. Wskazało je kolejno 80% i 74% respondentów. Bezprawne opublikowanie ich danych w internecie zaznaczyło 6% ankietowanych, a kradzież tożsamości – 7%. Przy tym pytaniu respondenci mogli wskazać więcej niż jedną odpowiedź.

SPOSOBY WYKORZYSTANIA POZYSKANYCH DANYCH*



*Respondenci mogli wskazać więcej niż jedną odpowiedź.

OKIEM EKSPERTA

Ten aspekt naszego badania okazał się zagadnieniem niezwykle ciekawym. Zdziwiło nas nieco, że zaledwie 26% osób przyznało, że ich prawo do ochrony danych osobowych zostało kiedyś naruszone. W dobie masowych kampanii mailingowych, telemarketingu oraz mnogości firm, oferujących różnego rodzaju bazy danych, nie zawsze właściwie zweryfikowanych, na sprzedaż i do wynajęcia (np. w celu jednorazowego przeprowadzenia jakiejś kampanii reklamowej), taki wynik wydaje się przynajmniej zaniżony. W naszej ocenie może to wynikać z tego, że jeszcze nie do końca zdajemy sobie sprawę z naszych praw w zakresie ochrony swojej prywatności. Wniosek ten zdaje się potwierdzać fakt, że niemal 60% osób, których dane zostały skradzione czy bezprawnie udostępnione, w żaden sposób na to nie zareagowało.

Pamiętajmy, że zgodnie z art. 32.1 ustawy o ochronie danych osobowych mamy prawo do kontroli przetwarzanych danych, które nas dotyczą, w tym również do otrzymania informacji, w jaki sposób zostały pozyskane oraz do wniesienia sprzeciwu wobec ich przetwarzania.

BEZPŁATNE PORADY

prawne i informatyczne z zakresu ochrony danych osobowych.

[ODO24.pl/pomoc](https://odo24.pl/pomoc)



Przetwarzanie danych osobowych w firmach i instytucjach.



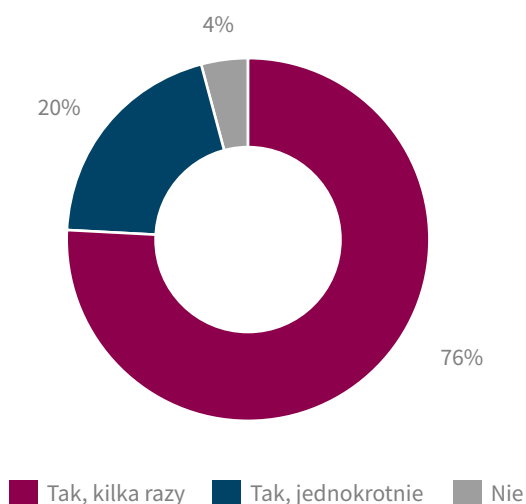
Znakomita większość przeszkolona, ale chce dowiedzieć się więcej.

Według różnych badań, największym ryzykiem dla skutecznej ochrony danych, w tym również danych osobowych jest... człowiek. Nawet 80% incydentów w różnego rodzaju firmach i instytucjach spowodowanych jest błędem, niedopatrzeniem lub po prostu nieświadomością pracownika. Zapytaliśmy więc samych pracowników, jak oceniają swoje przygotowanie do przetwarzania danych osobowych.

› Szkolenia

Zdecydowana większość respondentów z grupy pracowników, przetwarzających dane osobowe deklaruje, że przed przystąpieniem do pracy została przeszkolona z zasad ich ochrony. Co więcej, aż **76% grupy została przeszkolona więcej niż jeden raz!** Warto jednak zwrócić uwagę, że znaleźli się również tacy, którzy nie przeszli ani jednego szkolenia...

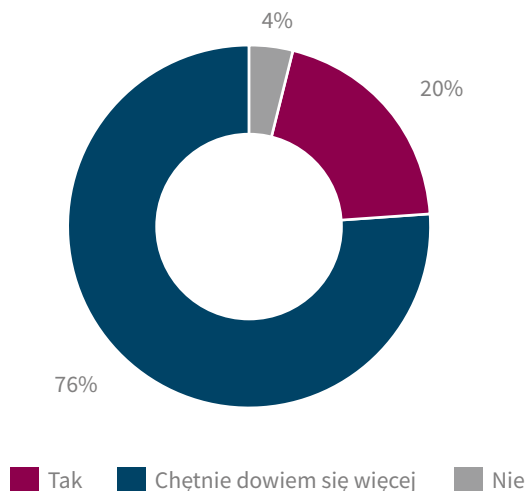
CZY ZOSTAŁEŚ PRZESZKOLONY Z OCHRONY DANYCH OSOBOWYCH?



› Wiedza

Dla porównania i zweryfikowania pytania o szkolenia, zapytaliśmy tych samych respondentów o to, jak oceniają swoją wiedzę z zakresu ochrony danych osobowych. Okazało się, że ilość osób, które uznały, że ich wiedza jest niewystarczająca, jest porównywalna z ilością osób, które nie zostały przeszkolone – 4%. 20% osób określiła swoją wiedzę jako wystarczającą, a pozostałe **76% wykazało chęć dalszego szkolenia**, mimo tego, że szkoleni już byli.

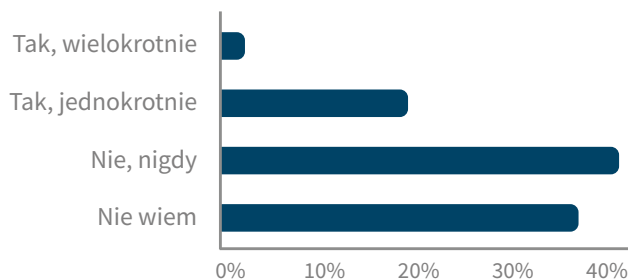
CZY MASZ WYSTARCZAJĄCĄ WIEDZĘ Z ZAKRESU OCHRONY DANYCH OSOBOWYCH?



› Incydenty

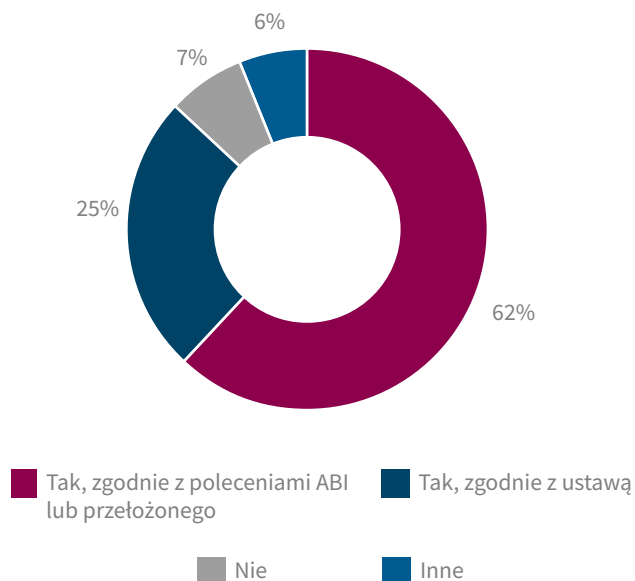
Zbadaliśmy również temat incydentów związanych z danymi osobowymi w firmach. Co ciekawe, aż **42% respondentów twierdzi, że w ich organizacji taki incydent nigdy nie miał miejsca!** 37% ankietowanych nie ma na ten temat wiedzy, a do wielokrotnych incydentów w swoich firmach czy instytucjach przyniosło się 2%.

INCYDENTY NARUSZENIA BEZPIECZEŃSTWA DANYCH



Spośród 20% organizacji, w których jednokrotnie lub wielokrotnie dochodziło do incydentów, **w zdecydowanej większości przypadków (87%) procedury bezpieczeństwa zadziałały prawidłowo** – postępowano zgodnie z poleceniami przełożonych lub administratorów bezpieczeństwa informacji (62%) albo też zgodnie z wytycznymi ustawy o ochronie danych osobowych (25%). W 7% przypadków nie podjęto żadnych kroków.

CZY W ZWIĄZKU Z INCYDENTEM ZOSTAŁY
W ORGANIZACJI PODJĘTE JAKIEŚ KROKI?



SZKOLENIA

- otwarte
- zamknięte
- e-learning



[ODO24.pl/szkolenia](https://odo24.pl/szkolenia)

OKIEM EKSPERTA

Okazuje się, że świadomość zasad ochrony danych osobowych nie jest w firmach i instytucjach tak mała, jak mogłoby się początkowo wydawać. Aż 76% pracowników, którzy na co dzień przetwarzają dane osobowe deklaruje, że zostali przeszkoleni z tego zakresu więcej niż raz. Pozytywnym zaskoczeniem jest to, że 76% przeszkolonych pracowników wyraziła chęć dalszego poszerzania swojej wiedzy w tym zakresie, co może świadczyć o tym, że zdają sobie sprawę z pewnych braków i ze względu na wagę tematu, chcieliby je jak najszybciej uzupełnić.

Warto podkreślić, że budowanie kompetencji pracowników jest kluczowym aspektem bezpieczeństwa – w przypadku 87% zaistniałych incydentów, procedury bezpieczeństwa zostały uruchomione i zadziałały prawidłowo.

System budowania kompetencji administratora bezpieczeństwa informacji

- szkolenie
- warsztaty
- egzamin

[ODO24.pl/system](https://odo24.pl/system)

Administrator bezpieczeństwa informacji (ABI)



78% ABI współdzieli
swoje obowiązki
z innymi zadaniami.

Administrator bezpieczeństwa informacji to osoba powołana przez administratora danych (zarówno spośród personelu wewnętrznego jak i spoza organizacji), odpowiedzialna za prowadzenie rejestru zbiorów danych osobowych oraz zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:

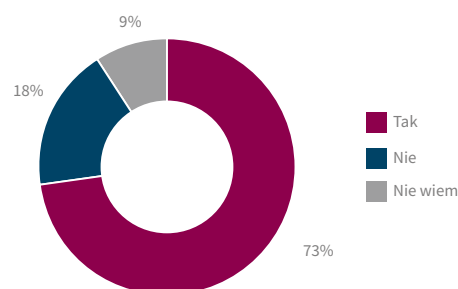
- sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,
- nadzorowanie opracowania i aktualizowania dokumentacji przetwarzania danych osobowych oraz przestrzegania określonych w niej zasad,
- zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

Od 1 stycznia 2015 r. powołanie ABI jest uprawnieniem, a nie obowiązkiem administratora danych.

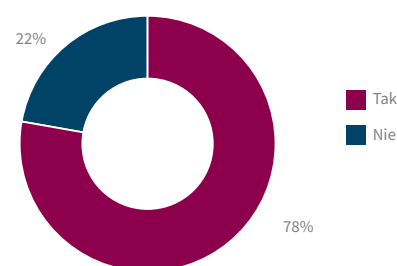
› ABI w organizacji

73% respondentów odpowiedziało, że w przedsiębiorstwie lub instytucji, w której pracują, **został powołany administrator danych osobowych**. 9% nie ma na ten temat wiedzy, a w 18% przypadków ABI nie został powołany. Wśród powołanych ABI, **aż 78% łączy swoją funkcję z innymi obowiązkami**.

ABI W ORGANIZACJI

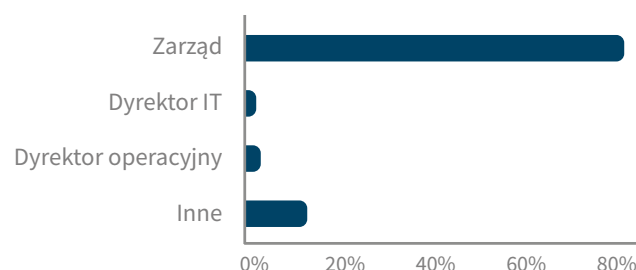


ŁĄCZENIE FUNKCJI ABI Z INNYMI OBOWIĄZKAMI



Zdecydowana większość powołanych ABI – **81% – podlega w swojej organizacji bezpośrednio zarządowi**. Dużo mniej zapytanych ABI wskazała jako swoich przełożonych dyrektorów IT (2%) i dyrektorów operacyjnych (3%).

PODLEGŁOŚĆ SŁUŻBOWA ABI

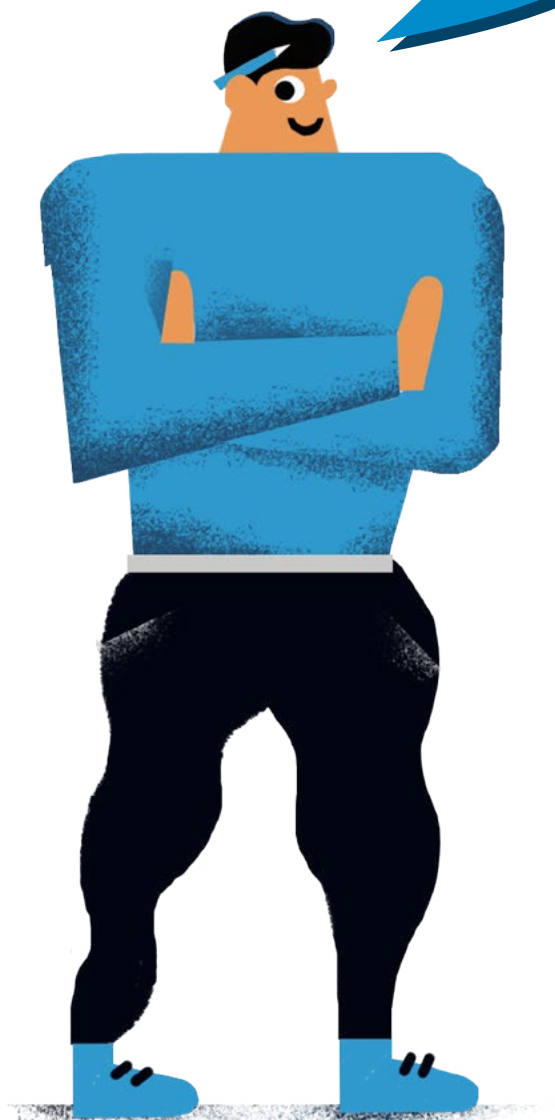


OKIEM EKSPERTA

Z przeprowadzonego badania wynika, że w zdecydowanej większości przypadków (73%) rdzeniem systemu ochrony danych osobowych jest powołany administrator bezpieczeństwa informacji. Pozwala to sądzić, iż organizacje zaczynają przykładać coraz większą wagę do ochrony przetwarzanych przez siebie danych osobowych, tworząc zręby architektury bezpieczeństwa informacji. Uzasadnionym pytaniem jest natomiast efektywność ABI. Ponad 80% z nich łączy bowiem swoją funkcję z innymi obowiązkami, realizowanymi w ramach organizacji. Ustawa o ochronie danych osobowych nie zabrania tego, ale podkreśla, że wykonywanie innych obowiązków nie powinno naruszyć prawidłowego wykonywania zadań ABI oraz, że ABI powinien być podległy bezpośrednio administratorowi danych. I rzeczywiście, przeprowadzone badania wykazały, że 80% ABI podlega bezpośrednio kierownictwu organizacji. To dobry sygnał, gdyż dzięki temu są oni dość niezależni i mogą skutecznie wykonywać powierzone im zadania.

Warto zauważyć, że ABI staje się widoczny w organizacji uczestnicząc w zarządzaniu incydentami bezpieczeństwa. W przypadku złożonej struktury i dużej liczby pracowników, celowe jawi się delegowanie części obowiązków ABI (np. w zakresie bieżącego nadzoru nad przestrzeganiem zapisów przyjętej w organizacji dokumentacji przetwarzania danych osobowych) na kierowników poszczególnych jednostek organizacyjnych lub lokalizacji zamiejscowych. Większe organizacje powinny rozważać powoływanie zastępców ABI.

Opinie na temat
nowelizacji ustawy
o ochronie danych
osobowych ze
stycznia 2015 r.



Nowelizacja bodźcem
do poszukiwania wiedzy,
potrzeba kampanii
informacyjnej, egzamin
dla ABI?

W ramach dodatkowego pytania otwartego zapytaliśmy respondentów o opinię na temat styczniowej nowelizacji ustawy o ochronie danych osobowych. Okazuje się, iż większość osób, które zechciały na nie odpowiedzieć, **pozytywnie ocenia wprowadzone zmiany**.

Respondenci zwrócili uwagę przede wszystkim na takie korzyści jak **zwolnienie z obowiązku rejestracji zbiorów w GIODO** w przypadku powołania w firmie administratora bezpieczeństwa informacji (ABI), a także na **dookreślenie roli ABI w organizacji**. Osoby, które mają do czynienia z międzynarodową wymianą danych osobowych, doceniły również **ułatwienie przekazywania danych do państw trzecich** – przed nowelizacją, w ich odczuciu, procedury były zbyt skomplikowane i trwały zbyt długo.

Co warto podkreślić, wielu respondentów jest zadowolonych, że **nowelizacja niejako zmusiła przedsiębiorców do zainteresowania się tematyką ochrony danych osobowych**. Zdaniem niektórych, część przedsiębiorców i decydentów w instytucjach publicznych przy okazji nowelizacji, pierwszy raz miała okazję usłyszeć, że ochrona danych jest ich prawnym obowiązkiem.

Niemniej to, że nowelizacja została oceniona dość pozytywnie, nie oznacza, że w odpowiedziach nie pojawiły się żadne wątpliwości. Bardzo wiele osób zwróciło uwagę na to, że **w ślad za nowelizacją ustawy nie poszła żadna kampania informacyjna**. Zdaniem respondentów świadomość społeczna, zarówno przeciętnego Kowalskiego, jak też kadr zarządzających, jest zdecydowanie zbyt niska, abyśmy mieli poczucie, że dane, jakie przekazujemy poszczególnym firmom czy instytucjom, są w pełni bezpieczne. Wśród sugestii rozwiązań tego problemu pojawiły się obowiązkowe

szkolenia pracowników różnych szczebli, ogólnopolska kampania informacyjna w mediach czy też specjalne infolinie obsługiwane przez ekspertów.

Uwagę zwróciła też kwestia ABI i jego miejsca w organizacji. Szczególne wątpliwości budzi ABI, który jest jednocześnie pracownikiem danego przedsiębiorcy i poza funkcją ABI wypełnia również inne obowiązki. Zdaniem osób, które zwróciły na to uwagę, **ABI będący jednocześnie pracownikiem to potencjalny problem z podległością służbową, a także z nadmiarem obowiązków**. W efekcie ochrona danych może spadać na ostatnie miejsce w hierarchii zadań takiego pracownika.

W przypadku ABI zwrócono też uwagę na brak informacji w ustawie na temat sposobów weryfikowania jego wiedzy. Pojawiły się głosy, że być może rozwiązaniem mógłby być wiarygodny egzamin, dający uprawnienia do pełnienia tej funkcji.

Co prawda w zdecydowanej mniejszości, ale wśród odpowiedzi pojawiły się również głosy krytyczne. Zdaniem niezadowolonych z nowelizacji, skupia się ona głównie na wielu niepotrzebnych obowiązkach dokumentacyjno-technicznych zamiast dostosować prawo do współczesnych realiów. Jak podkreślają, skuteczna ochrona danych wymaga zdecydowanie głębszych zmian. Przykładowo, warto rozważyć ograniczenie ilości danych, które jesteśmy zmuszeni przekazywać różnego rodzaju firmom i instytucjom, np. pracodawcy przy zawieraniu umowy o pracę. Ktoś inny wspomniał też o konieczności udostępnienia GIODO lepszych narzędzi do zwalczania nieuczciwych praktyk. Obecnie nakładane kary przez część osób zostały uznane za zdecydowanie niewystarczające.

dla

ODO24.pl/dlaABI

ABI

- wsparcie
- audyt
- dokumentacja
- szkolenia
- warsztaty
- egzamin

Charakterystyka respondentów

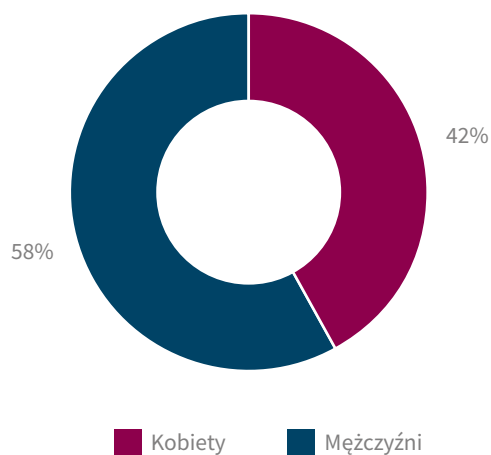


Płeć,
miejsce zamieszkania,
sytuacja zawodowa,
obszar zatrudnienia.

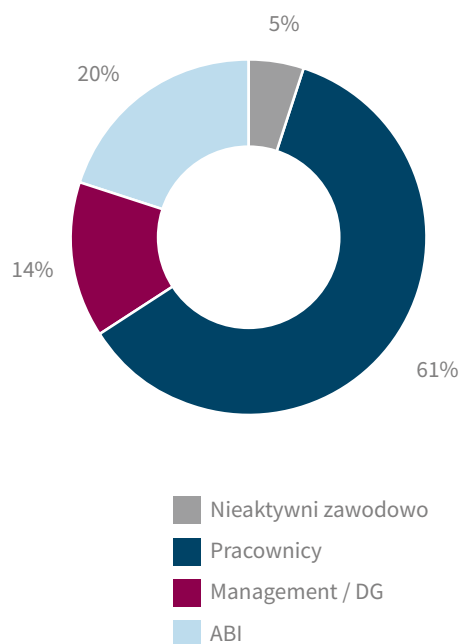
Łącznie w naszej ankiecie przepytaliśmy 1072 respondentów – 626 mężczyzn i 446 kobiet.

Największą grupę spośród badanych stanowili mieszkańcy dużych miast – 33% oraz osoby zatrudnione w administracji publicznej – 23%, usługach – 13% oraz branży IT – 13%.

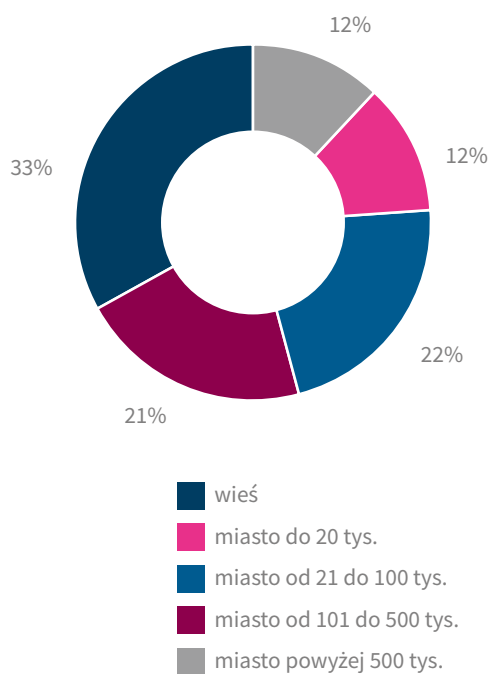
PŁEĆ



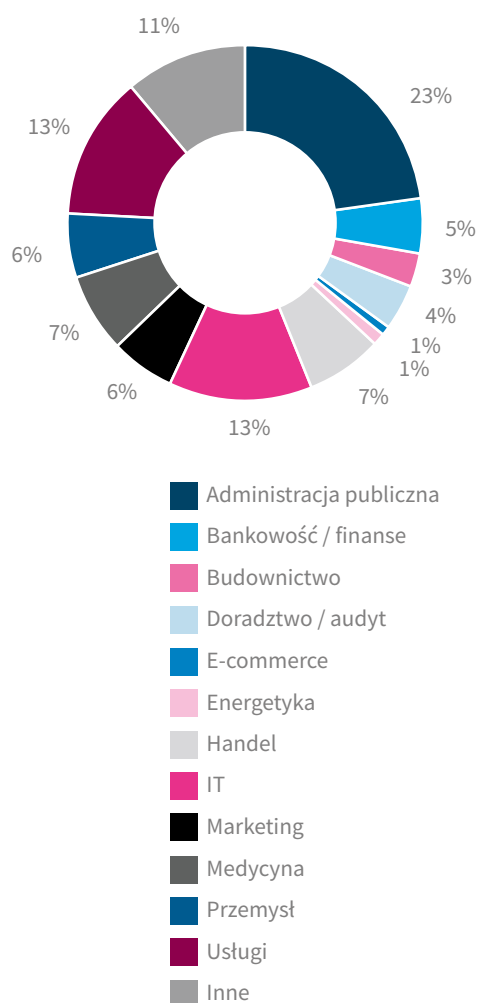
SYTUACJA ZAWODOWA



MIEJSCE ZAMIESZKANIA



OBSZAR ZATRUDNIENIA



Podstawowe zasady ochrony danych osobowych

- Traktuj dane osobowe innych tak, jak chciałbyś, by były traktowane Twoje.
- Po zakończeniu pracy, usuwaj dane osobowe z zasięgu wzroku i dłoni innych.
- Blokuj komputer za każdym razem gdy odchodzisz od stanowiska pracy.
- Jeżeli nie jesteś pewien, z kim rozmawiasz, nigdy nie podawaj danych osobowych przez telefon.
- Zanim wyślesz maila, uważnie sprawdź, czy właściwie wpisałeś adres odbiorcy.
- Wysyłając maile do wielu odbiorców, zawsze wpisuj ich adresy w kopii ukrytej.
- Pracując na danych osobowych, korzystaj tylko z hotspotów zabezpieczonych hasłem.
- Nie wyrzucaj dokumentów zawierających dane osobowe do śmietnika – korzystaj z niszczarek.
- Nie pozostawiaj osób nieupoważnionych z danymi osobowymi bez nadzoru.
- Regularnie zmieniaj swoje hasła dostępowe, nikomu ich nie przekazuj i nie zapisuj w widocznych miejscach.

System bezpieczeństwa informacji

Tel. 22 740 99 99