FUNDACJA
WIEDZA TO BEZPIECZEŃSTWO

CO WIEMY O OCHRONIE DANYCH

RAPORT 2017

WTB.org.pl

› Spis treści

Wprowadzenie 3

Jakie urządzenia są najpopularniejsze? 4

Czy chronimy dane na komputerach i laptopach? 6

Jak zabezpieczamy urządzenia mobilne? 9

Jak postrzegamy zagrożenia dla danych osobowych? 12

Jak traktujemy naruszenia prawa do ochrony danych osobowych? 16

RODO coraz bliżej. Czy widać to w organizacjach? 20

Charakterystyka uczestników badania 24

FUNDACJA
WIEDZA TO BEZPIECZEŃSTWO

Fundacja Wiedza To Bezpieczeństwo to inicjatywa osób zawodowo zajmujących się bezpieczeństwem informacji, łączymy wiedzę, pasję i doświadczenie z różnych dyscyplin – m.in. prawa, informatyki, zarządzania. Istniejemy po to, by promować znaczenie bezpieczeństwa informacji, budować świadomość społeczeństwa - zarówno osób prywatnych, jak i przedsiębiorstw - w zakresie posiadanych danych i ich znaczenia w codziennym życiu, a w przypadku firm w osiąganiu przewagi konkurencyjnej.

› *Raport*

Powstał na podstawie badania przeprowadzonego w dniach 01.03.2017 – 05.04.2017 r.. Narzędziem badawczym była ankieta online, zamieszczona na stronie Internetowej: wtb.org.pl. Badaniem objęliśmy cztery grupy osób:

Grupa osób	Ilość ankiet
Nieaktywnych zawodowo w tym uczących się	299
Pracujący	526
Zarządzający firmami	141
Specjalizujących się w ochronie danych osobowych	370
Wszystkich ankietowanych	**1 326**

Autorzy
dr Paweł Mielniczek - prawnik i naukowiec specjalizujący się w prawie międzynarodowym, ochronie praw jednostki i prawie nowych technologii.

Leszek Kępa - Wiceprzewodniczący Rady Fundacji Wiedza To Bezpieczeństwo, ekspert ds. ochrony danych osobowych i bezpieczeństwa informacji.

Ilustracje
Karol Banach (karolbanach.com)

Projekt i skład
Radosław Zgódka (inpixel.pl)

Redakcja
Martyna Danielewicz (triplepr.pl)

ISBN: 978-83-948468-0-0

Warszawa, lipiec 2017 r.

› Szanowni Państwo

przedstawiamy wyniki badania świadomości społeczeństwa w zakresie ochrony danych osobowych. Fundacja Wiedza To Bezpieczeństwo zapytała ankietowanych, w jaki sposób chronią dane i jak oceniają ryzyko ich utraty.

Badanie pokazało, że Polacy są świadomi zagrożeń związanych z naruszeniem danych osobowych. Nie są natomiast pewni, jak się przed nimi zabezpieczyć i jak reagować w razie incydentu. Stąd aż 90% osób aktywnych zawodowo czuje potrzebę pogłębiania swojej wiedzy poprzez dedykowane szkolenie z ochrony danych osobowych.

Jedna trzecia wszystkich ankietowanych przynajmniej raz w życiu doświadczyła naruszenia prawa do prywatności. Ale tylko co dziesiąty ankietowany zgłosił to odpowiedniej instytucji, pozostali ignorują takie incydenty, dzięki czemu sprawcy czują się bezkarni i pozwalają sobie na więcej. Brak reakcji nie wynika jednak z braku świadomości zagrożenia, ankietowani po prostu nie wierzą, że to ma sens. Administratorzy bezpieczeństwa informacji (ABI) doskonale to wiedzą, a mimo to wciąż 32% z nich wątpi w sens zgłaszania takiego incydentu... Wskazuje to na niedostatki środków ochrony prawnej.

Zdaniem respondentów, jednym z największych zagrożeń dla prywatności są podmioty przetwarzające dane swoich własnych klientów, interesariuszy czy pracowników. Wiele z nich wciąż nie przykłada należytej uwagi do ochrony danych, co zdaje się potwierdzać fakt, że znakomita większość ABI obok ochrony danych osobowych i bezpieczeństwa informacji, wykonuje w swojej firmie także inne zadania.

Uczestników badania zapytaliśmy także o kwestie związane ze znajomością europejskiego rozporządzenia o ochronie danych osobowych (RODO, ang. GDPR) i wdrożenia jego przepisów w organizacjach. Zaledwie nieco ponad połowa kadry zarządzającej wie, jakie obowiązki na firmy nakłada ta regulacja. Co więcej, jeszcze mniej ABI (31%) wie, co będzie należało do zakresu ich obowiązków w przyszłym roku, po wejściu w życie RODO. Wyniki badania pokazują, że świadomość przepisów jest spora, co roku coraz większa, ale wciąż potrzebna jest w tym obszarze edukacja i budowanie świadomości.

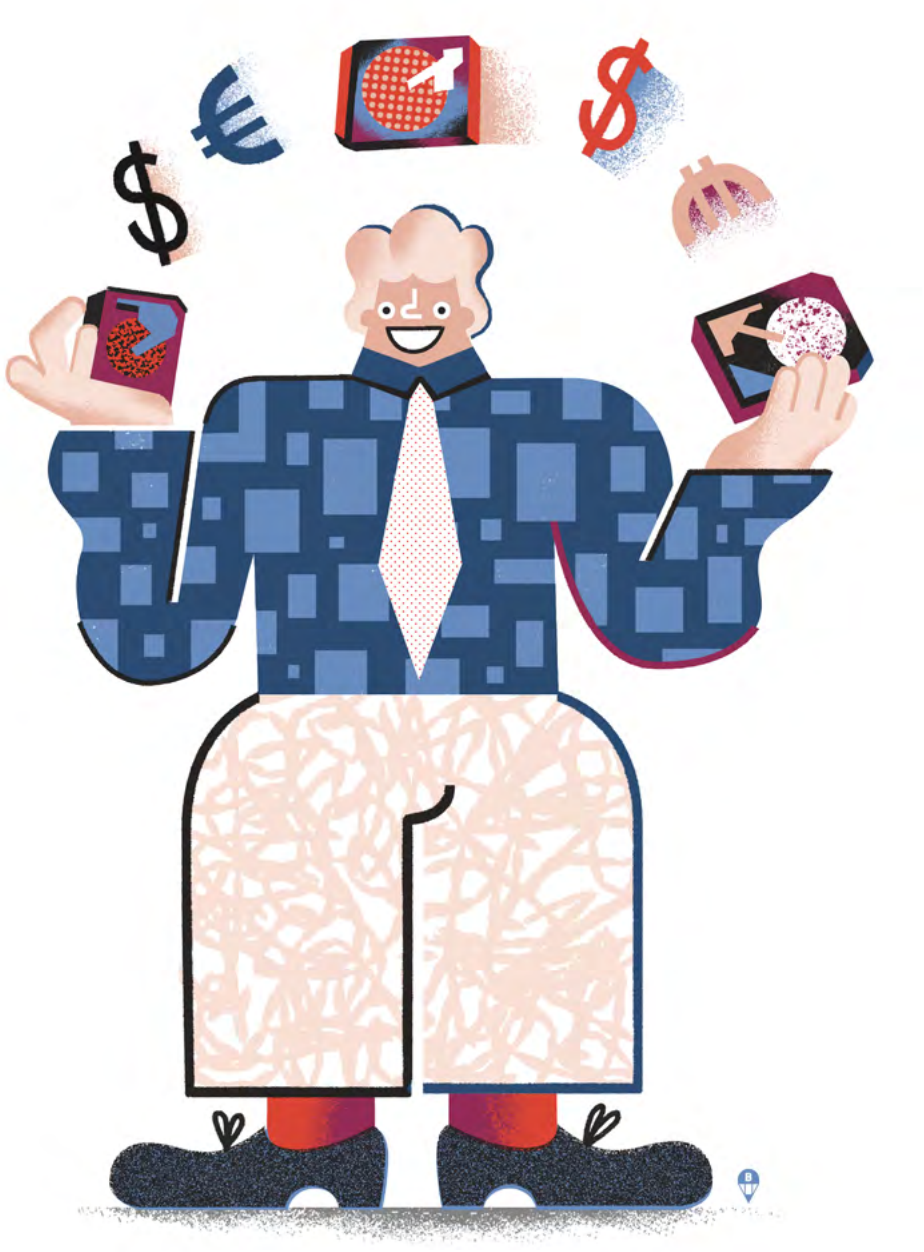
W raporcie znajdą Państwo podsumowanie przeprowadzonego przez nas badania oraz eksperckie komentarze dotyczące jego wyników. Zapraszamy do lektury!

Maciej Kaczmarski

Przewodniczący Rady
Fundacja Wiedza To Bezpieczeństwo

Jakie urządzenia są najpopularniejsze?

Najpopularniejsze pozostają laptopy i smartfony. Ochrona danych stopniowo rozszerza się na tzw. Internet rzeczy.

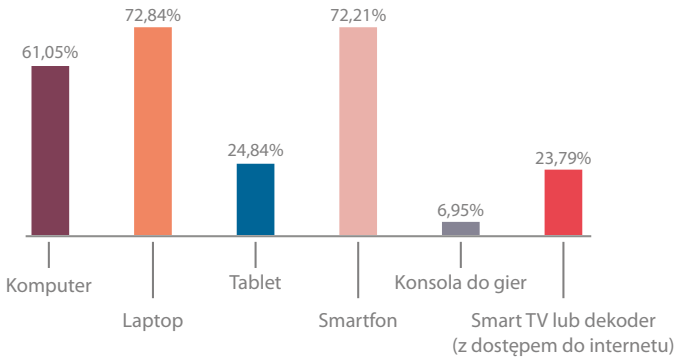


Jak pokazało przeprowadzone przez nas badanie, aż 96% ankietowanych korzysta z komputera lub laptopa, a 72% także ze smartfonu.

Najpopularniejszymi urządzeniami, z których na co dzień korzystają respondenci jest laptop – 73% i smartfon – 72%. W dalszej kolejności wybierane są komputery – 61%, tablety – 25% i telewizory smart lub dekodery (z podłączeniem do Internetu) – 24% oraz konsole do gier – 7%.

Osoby nieaktywne zawodowo lub uczące się korzystają przede wszystkim ze smartfonów – 75% i laptopów – 68%. Podobnie kształtują się preferencje pracowników oraz osób prowadzących działalność gospodarczą lub zarządzających organizacją – one również zdecydowanie najchętniej korzystają z laptopów – odpowiednio 74% i 77% oraz smartfonów – odpowiednio 72% i 74%. Inaczej wygląda sytuacja w grupie obejmującej osoby zajmujące się ochroną danych osobowych lub ochroną informacji, w niej najpopularniejszymi urządzeniami są komputery i laptopy – po 72% oraz smartfony – 70%.

NAJPOPULARNIEJSZE URZĄDZENIA



KOMENTARZ FUNDACJI WTB

Bardzo ciekawy jest rosnący trend związany z urządzeniami elektronicznymi, z których korzystają respondenci. Wydawałoby się, że urządzenia przenośne będą wypierać powoli komputery stacjonarne, ale wyniki badania pokazały, że ankietowani, mimo że używają laptopa, to aż w 61% przypadków korzystają także z komputera stacjonarnego. Z komputerów korzystają przede wszystkim pracownicy i właściciele firm. Ma na to wpływ czynnik ekonomiczny, tj. niższe koszty sprzętu.

Wzrasta wykorzystanie przedmiotów tworzących tzw. „Internet rzeczy" (ang. Internet of things). Choć w tym zakresie nasze badanie objęło tylko telewizory i dekodery z podłączeniem do Internetu, to już na tej niewielkiej próbie widać ich rosnącą popularność. Warto zwrócić uwagę na odpowiednie zabezpieczenie takich sprzętów, zwłaszcza w kontekście niedawnych doniesień medialnych o „podsłuchujących telewizorach" Samsunga, które wszystkie usłyszane dialogi wysyłały do analizy do innej firmy w celu wyłowienia poleceń dla urządzenia. Takie sytuacje pokazują, jak istotne jest włączenie bezpieczeństwa już na etapie projektowania urządzenia. Warto w tej sytuacji wspomnieć o tym, że RODO wprowadza właśnie taki wymóg.

Czy chronimy dane na komputerach i laptopach?

Stosowanie haseł staje się tak oczywiste jak zamykanie drzwi na klucz. Wciąż mało popularne jest szyfrowanie danych.

Stosowanie haseł, używanie programu antywirusowego i szyfrowanie to najczęściej stosowane sposoby chronienia danych osobowych na urządzeniach desktopowych. Z naszego badania wynika, że tylko 3% z nas nie stosuje żadnych zabezpieczeń na swoich komputerach i laptopach, a 76% korzysta z więcej niż jednego.

› Stosowanie haseł

Z haseł, które są najprostszą do wykorzystania formą zabezpieczenia danych na komputerach i laptopach, korzysta aż 84% respondentów. Ten sposób jest najbardziej popularny wśród osób zawodowo zajmujących się ochroną danych osobowych (95%) oraz prowadzących działalność gospodarczą lub zarządzających organizacjami (92%). Jest on również chętnie wykorzystywany przez pracowników (84%). Najrzadziej z tego typu zabezpieczenia korzystają uczniowie i studenci oraz bezrobotni. Robi to tylko 66% z nich.

› Używanie programu antywirusowego

Programy antywirusowe są drugim w kolejności najpopularniejszym zabezpieczeniem. Na komputerach i laptopach korzysta z nich 82% ankietowanych. Najczęściej stosowane są przez profesjonalistów zajmujących się na co dzień ochroną danych osobowych (90%) oraz przez osoby aktywne zawodowo (82%). Z tego sposobu chronienia komputerów i laptopów korzysta również ponad trzy czwarte (76%) kadry zarządzającej i właścicieli firm oraz nieznacznie mniej (69%) osób nieaktywnych zawodowo lub uczących się.

OKIEM EKSPERTA

Hasło to podstawowy element bezpieczeństwa systemów i aplikacji informatycznych. Liczba znaków czy złożoność konstrukcji hasła wpływa na wzrost jego bezpieczeństwa. Obecnie hasła uważane za bezpieczne to takie, które składają się z co najmniej 12 znaków zawierających wielkie litery, cyfry i znaki specjalne. Należy jednak uważać, aby hasło nie było słownikowe czy skojarzeniowe tzn. aby litery nie tworzyły słów powszechnie używanych oraz nie miały w swej konstrukcji imion, nazwisk czy nazw własnych. Dostępne są również rozwiązania techniczne podwyższające poziom bezpieczeństwa tj. hasło przesyłane SMS-em, token czy klucz SSL. Warto też rozważyć stosowanie uwierzytelnienia wieloskładnikowego np. login, hasło oraz pin przesłany SMS-em. Należy pamiętać, że hasło jest na tyle bezpieczne, na ile jego właściciel posługuje się nim odpowiedzialnie. Przykładowo, zapisanie hasła na kartce, czy wpisywanie go w obecności innych osób, stwarza niebezpieczeństwo przechwycenia.

Maciej Jurczyk
Inżynier ds. bezpieczeństwa informacji, ODO 24 sp. z o.o.

KOMENTARZ FUNDACJI WTB

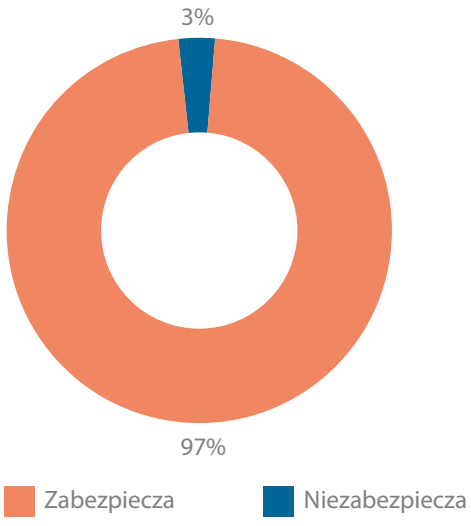
Programy antywirusowe, które zapewniają ochronę przed złośliwym oprogramowaniem są bardzo popularne wśród użytkowników sprzętu elektronicznego. W organizacjach są one obowiązkowe - takie wymaganie stawia rozporządzenie do ustawy o ochronie danych osobowych, ale tzw. antywirusy powinny być także stosowane na prywatnych urządzeniach.

Na rynku dostępna jest szeroka gama darmowego i prostego w instalacji oprogramowania antywirusowego, w tym także dla urządzeń z systemem OSX lub Linux.

› Szyfrowanie

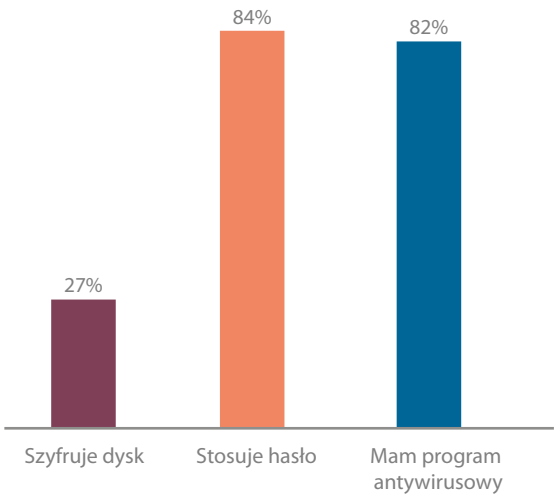
Tylko 27% ankietowanych szyfruje dyski używanych komputerów i laptopów. Ten sposób zabezpieczenia danych jest najrzadziej stosowany przez osoby niepracujące (8%), częściej natomiast wykorzystują go pracownicy (23%). Szyfrowanie wykorzystuje prawie połowa osób (48%) zawodowo zajmujących się ochroną danych osobowych.

ILE OSÓB ZABEZPIECZA SWOJE KOMPUTERY?



Co ciekawe nieznacznie więcej osób szyfruje dysk z grupy obejmującej kadrę zarządzającą organizacji (50%).

POPULARNOŚĆ STOSOWANYCH ZABEZPIECZEŃ - KOMPUTERY



KOMENTARZ FUNDACJI WTB

Szyfrowanie należy implementować wtedy, gdy przechowuje się na danym urządzeniu takie dane, których przejęcie przez osoby postronne może osobie prywatnej albo organizacji zaszkodzić.

Z badania wynika, że szyfrowanie dysku nie jest zbyt powszechne. Przede wszystkim nie jest tak łatwo dostępne, jak programy antywirusowe. Najczęściej wymaga kupna licencji i jest nieco trudniejsze w samodzielnej instalacji. Najprawdopodobniej większość użytkowników uważa, że hasło wystarczająco dobrze chroni ich zasoby znajdujące się na urządzeniach. Szyfrowanie dysków w komputerach stacjonarnych spotyka się niezmiernie rzadko – z uwagi na to, że są mniej narażone na utratę danych w stosunku do urządzeń mobilnych.

Dobrą wiadomością jest zaś, że kadra kierownicza docenia i rozumie potrzebę szyfrowania danych, aby zabezpieczyć je przed dostępem osób niepowołanych i stosuje szyfrowanie częściej nawet niż specjaliści od ochrony danych osobowych.

Jak zabezpieczamy urządzenia mobilne?

Wybór między mocnym hasłem, krótkim PIN-em, a wzorem na ekranie często zależy od szybkości wpisywania. Alternatywą stają się zabezpieczenia biometryczne.

Z badania wynika, że 94% z nas zabezpiecza swoje smartfony, a 91% tablety. Najczęściej chronimy je używając: PIN-u (na tablecie – 32%, na smartfonie – 34%), mocnego hasła (na tablecie – 27%, na smartfonie – 12%), wzoru na ekranie (na tablecie – 23%, na smartfonie – 26%). Ponadto wykorzystujemy także zabezpieczenia biometryczne (na tablecie – 9%, na smartfonie – 16%) oraz blokadę ekranu urządzenia. (na tablecie – 8%, na smartfonie – 11%).

› PIN

Stosowanie PIN-u jest najpopularniejszym sposobem zabezpieczenia smartfonu dla osób aktywnych zawodowo (35%) jak i bezrobotnych lub uczących się (31%). Korzysta z niego także co piąty (22%) właściciel lub zarządzający firmą. Zaskakuje, że aż 39% respondentów z grupy specjalistów na co dzień zajmujących się ochroną danych osobowych stosuje na smartfonie PIN zamiast mocniejszych zabezpieczeń.

PIN to także często wykorzystywane zabezpieczenie na tabletach. Stosuje go 38% kadry zarządzającej, 34% pracowników, 30% bezrobotnych i uczących się oraz 23% osób zajmujących się zawodowo ochroną danych osobowych.

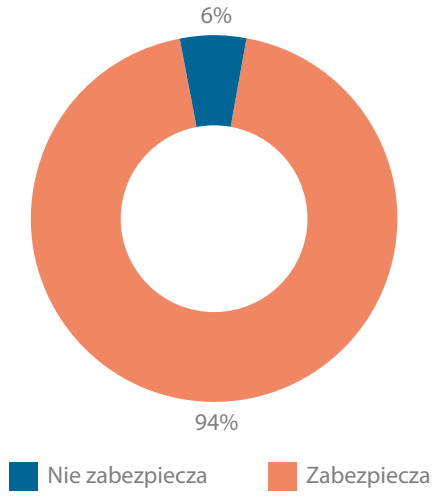
› Mocne hasło

Hasło składające się zarówno z małych i dużych liter oraz cyfr, a także znaków specjalnych wykorzystuje na smartfonach: 19% kadry zarządzającej, 16% osób niepracujących lub uczących się, 12% pracowników i 7% specjalistów z zakresu danych osobowych.
Na tabletach mocne hasło używa, podobnie jak na smartfonach, 22% pracujących i 20% bezrobotnych, a znacznie więcej kadry zarządzającej oraz osób zajmujących się ochroną danych osobowych (odpowiednio 38% i 41%).

› Wzór na ekranie

Poprzez stosowanie wzoru na ekranie, smartfon chroni: 29% osób nieaktywnych zawodowo lub uczących się, po 26% pracowników i kadry zarządzającej oraz 24% specjalistów z zakresu ochrony danych.
Na tablecie ten sposób zabezpieczenia wykorzystuje: 30% bezrobotnych, 24% pracowników i 27% osób zajmujących się zawodowo ochroną danych. Żaden z respondentów badania należących do grupy osób prowadzących działalność gospodarczą lub zarządzających organizacją nie wskazał tej formy chronienia tabletu.

ILE OSÓB ZABEZPIECZA SWOJE SMARTFONY

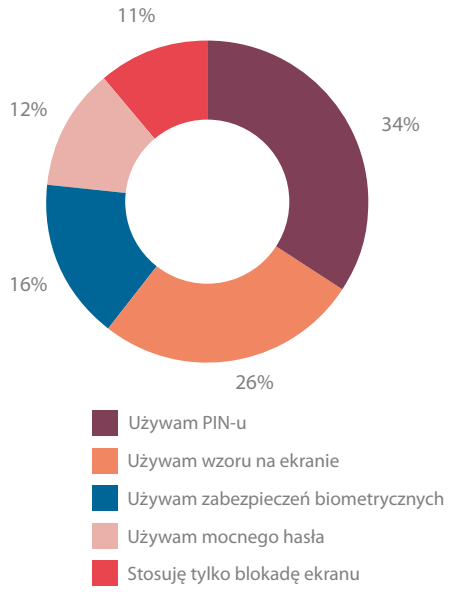


KOMENTARZ FUNDACJI WTB

Pamiętajmy, że nie chronimy urządzeń, ale informacje, jakie na nich przechowujemy. Im ważniejsze informacje i im większą szkodę może wyrządzić ich wyciek, tym lepsze i mocniejsze zabezpieczenia trzeba stosować. Jednak takie zabezpieczenia powinny być jednocześnie praktyczne i nie powinny utrudniać codziennej pracy – doskonałym przykładem są mocne hasła na urządzeniach mobilnych. Wpisanie ośmioznakowego hasła, które składa się z cyfr, małych i wielkich liter oraz znaków specjalnych na laptopie nie stanowi żadnej trudności, wpisanie go na tablecie jest już pewnym wyzwaniem, zaś na telefonie komórkowym, który ma mniejszy ekran i niewielką klawiaturę – stanowi sporą trudność. Nie dziwi, że użytkownicy telefonów komórkowych chętniej korzystają z alternatywnych metod takich jak wzór (pattern) czy biometria.

Ciekawostką jest to, że specjaliści od ochrony danych osobowych najchętniej wybierają PIN, może to wynikać z faktu, że ich urządzenia są chronione przez tzw. system MDM (ang. mobile device management) – wówczas telefon jest chroniony najczęściej za pomocą PIN-u, a firmowe dane znajdują się w bezpiecznym kontenerze, do którego dostęp jest możliwy po podaniu „mocnego" hasła.

STOSOWANE ZABEZPIECZENIA - SMARTFONY



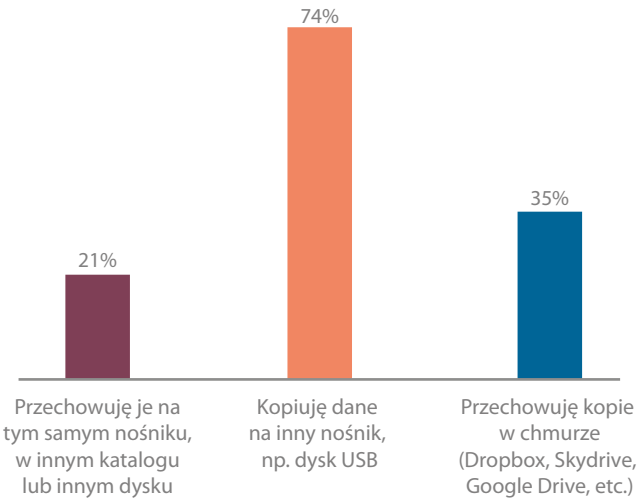
› *Kopie danych*

Na pytanie dotyczące wykonywania kopii zapasowych swoich danych pozytywnie odpowiedziało aż 8 na 10 ankietowanych. 44% osób kopiuje dane sporadycznie, a 37% robi to regularnie. Jeszcze lepsze wyniki zostały zanotowane w grupie osób zawodowo zajmujących się ochroną danych osobowych – aż 95% wykonuje kopie swoich danych, w tym 70% regularnie.

Osoby, które wzięły udział w badaniu, najczęściej kopiują dane na zewnętrzny nośnik np. USB – 74%, a w dalszej kolejności przechowują kopie w chmurze – 35% oraz zapisują je na tym samym nośniku, ale w innym katalogu lub na innym dysku – 21%. Najwięcej osób – 68% korzysta tylko z jednego sposobu kopiowania danych, z dwóch 27%, a z trzech zaledwie 5%.

Kopiowanie danych na zewnętrzny dysk było wskazywane jako sposób najczęściej stosowany przez osoby niepracujące lub uczące się (aż 84%) oraz zawodowo zajmujące się ochroną danych osobowych (83%). Najmniej popularną formą we wszystkich grupach jest kopiowanie danych na ten sam nośnik, ale w innym katalogu lub na innym dysku.

GDZIE NAJCZĘŚCIEJ ZAPISUJEMY KOPIE DANYCH



KOMENTARZ FUNDACJI WTB

W branży bezpieczeństwa mówi się, że są dwa rodzaje użytkowników: ci, którzy wykonują kopie zapasowe oraz ci, którzy będą to robić. Prawie każdy stracił kiedyś jakieś ważne dokumenty, zdjęcia, pliki, niezapisaną pracę magisterską. Warto pamiętać, że wcale nie trzeba stracić urządzenia, aby stracić dane. Czasami nawet „zawieszenie" edytora tekstu może sprawić, że zapisany dokument okaże się… pusty! Na takich błędach uczymy się i zaczynamy wykonywać kopie zapasowe, które pozwalają odzyskać utracone dane. Jesteśmy też coraz bardziej świadomi, że kopia na tym samym nośniku nie chroni naszych danych w wystarczającym stopniu.

Jak postrzegamy zagrożenia dla danych osobowych?

Korzyści oferowane przez cyfrowe usługi sprawiają, że często automatycznie podajemy dane osobowe, przymykając oko na zagrożenia.

Respondenci badania zapytani o to, jak oceniają ryzyko nieodwracalnej utraty swoich danych przede wszystkim odpowiadali, że jako średnie (45%) lub niskie (29%). Tylko 12% uznało je za wysokie, a 6% za bardzo wysokie. Co ciekawe 8% badanych stwierdziło, że ryzyko utraty lub uszkodzenia danych jest bardzo niskie.

Jeśli chodzi o ocenę ryzyka nieodwracalnej utraty danych w poszczególnych grupach, to najbardziej zbliżone do odpowiedzi ogółu badanych były odpowiedzi pracowników. 30% z nich oceniło, że ryzyko to jest niskie, 47%, że średnie, a 11% - że wysokie. Skrajne odpowiedzi – bardzo wysokie i bardzo niskie wskazało po 6% ankietowanych. Podobne odczucia mają także osoby nieaktywne zawodowo lub uczące się. Ankietowani z tej grupy ocenili ryzyko utraty danych następująco: średnie - 46%, niskie - 29%, wysokie i bardzo wysokie - po 9%, bardzo niskie - 7%.

Prawie połowa osób (47%) na co dzień zajmujących się ochroną danych osobowych określiło ryzyko jako średnie, a jedna trzecia (33%) jako niskie. Odpowiedzi „wysokie", „bardzo wysokie" i „bardzo niskie" wskazało odpowiednio 14%, 3% i 4% z nich.

Oceny osób zaliczających się do managementu były bardziej podzielone niż w pozostałych grupach. Respondenci określili ryzyko kolejno jako: średnie – 26%, bardzo niskie – 26%, wysokie – 23%, niskie – 21%, bardzo wysokie – 5%.

› *Kradzież danych*

Uczestnicy badania na podobnym poziomie określają zagrożenie kradzieżą danych oraz innymi możliwościami ich utraty. Większość ocenia je albo jako średnie, albo jako niskie (odpowiednio 46% i 28%). Dla pozostałych jest ono wysokie (12%), bardzo wysokie (6%) lub bardzo niskie (9%).

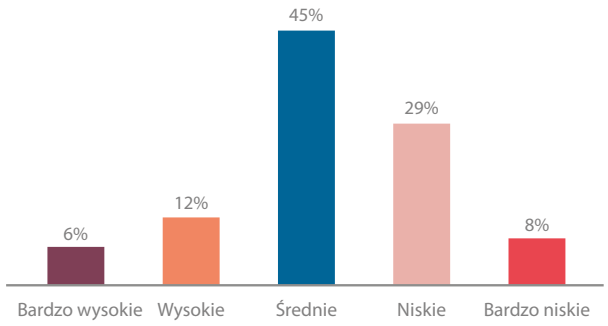
Ryzyko związane z kradzieżą danych jako wysokie lub bardzo wysokie (po 10%) oraz jako średnie (51%) ocenia zdecydowana część kadry zarządzającej. Tylko dla 15% jest ono niskie i 13% bardzo niskie.

W grupie, do której zaliczeni zostali ABI (Administratorzy Bezpieczeństwa Informacji) także dominowały odpowiedzi „średnie" i „niskie" (odpowiednio 44% i 29%). W dalszej kolejności wymieniane były: „bardzo niskie" (14%), „wysokie" (10%) i „bardzo wysokie" (3%).

Prawie połowa pracowników (48%) określiła ryzyko kradzieży jako średnie, a prawie jedna trzecia (30%) jako niskie. 10% osób zaliczanych do tej grupy oszacowało je zaś jako wysokie. Skrajne odpowiedzi - „bardzo wysokie" i „bardzo niskie" wskazało odpowiednio 6% i 7%.

Odpowiedzi osób niepracujących rozłożyły się zaś następująco: średnie – 36%, niskie – 29%, wysokie – 20%, bardzo wysokie lub bardzo niskie – po 7%.

JAK OCENIASZ RYZYKO UTRATY LUB KRADZIEŻY SWOICH DANYCH



OKIEM EKSPERTA

Rozwój usług opartych o transmisję danych za pośrednictwem Internetu spowodował, że chcąc ułatwić sobie życie instalując kolejną aplikację zgadzamy się na każdy zaproponowany przez usługodawcę warunek. Podajemy dane osobowe w sposób automatyczny, bardzo rzadko zastanawiając się nad ich losami. Z drugiej strony, na szczęście, w ostatnich latach nie mieliśmy do czynienia ze spektakularnymi przykładami naruszenia praw klientów czy konsumentów. Tak więc przytoczone wyniki specjalnie mnie nie dziwią. Paradoksalnie największe incydenty w zakresie nieprawidłowości w przetwarzaniu danych osobowych zanotowano w instytucjach, które stosują najbardziej rygorystyczne procedury bezpieczeństwa. Być może dość optymistycznie brzmiące odpowiedzi respondentów wynikają z zaufania do usługodawców i stosowanych przez nich metod ochrony informacji.

Maciej Buś
Prezes, Polskie Forum Call Center

› *Zagrożenia dla bezpieczeństwa danych osobowych*

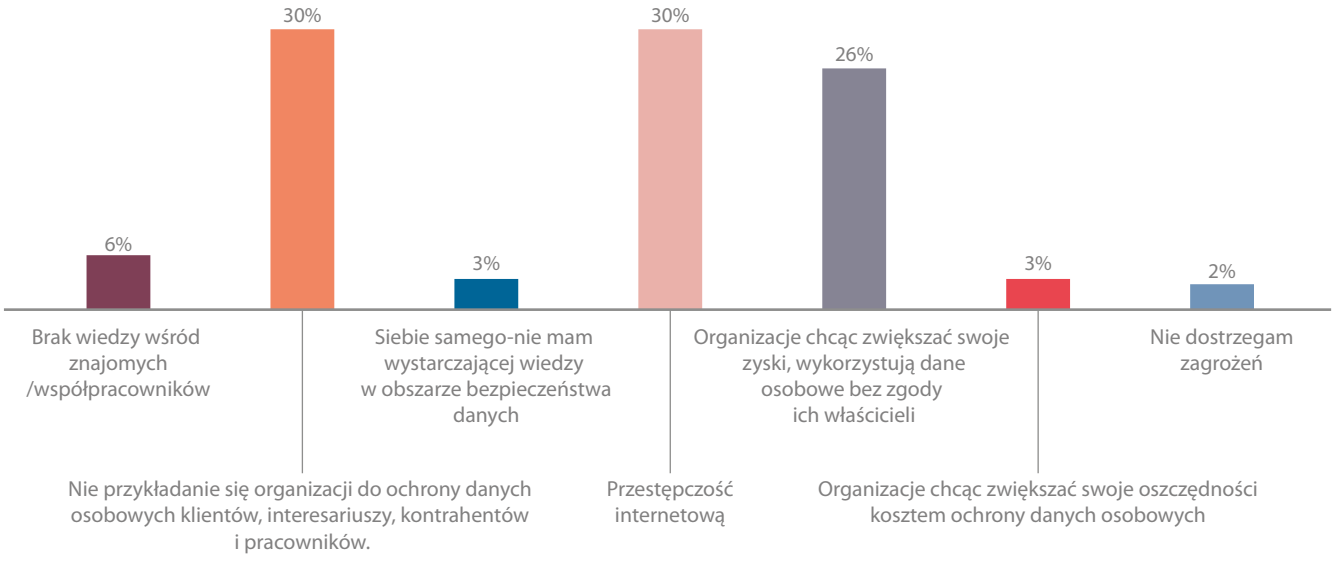
Dla respondentów największym niebezpieczeństwem są:

- organizacje, które chcą zwiększać swoje zyski, wykorzystując dane osobowe bez zgody osób, których dotyczą (26%);
- przestępczość internetowa (30%);
- nieprzywiązywanie dostatecznej uwagi przez różne podmioty do ochrony danych osobowych swoich klientów/interesariuszy, kontrahentów i pracowników (30%).

Zdecydowanie mniej badanych stwierdziło, że zagrożeniem dla ich danych są znajomi/współpracownicy oraz ich brak wiedzy w tym obszarze (6%) oraz organizacje chcące zwiększać oszczędności kosztem ochrony danych osobowych (3%). Część ankietowanych (3%) wskazała, że niebezpieczny jest dla nich także brak wystarczającej wiedzy w obszarze bezpieczeństwa danych. 2% osób nie dostrzega żadnych zagrożeń.

Bezrobotni najczęściej (41%) wskazywali, że zagrożeń dla bezpieczeństwa swoich danych upatrują w przestępczości internetowej. Podobnego zdania są także pracownicy (31%) oraz management (36%). Dla osób zawodowo zajmujących się ochroną danych osobowych największe zagrożenie stanowią podmioty, które nie przykładają się do ochrony danych osobowych zarówno swoich pracowników jak i klientów (52%). Jest to drugie niebezpieczeństwo zauważane przez pozostałe grupy, zaznaczyło je w ankiecie: po 25% bezrobotnych i pracowników oraz 33% kadry zarządzającej. Organizacje, które wykorzystują dane bez zgody ich właścicieli, aby zwiększyć swoje zyski, jako zagrożenie traktuje zaś: 23% osób nieaktywnych zawodowo lub uczących się, 29% pracowników, 21% managementu oraz 19% ABI.

CO UWAŻASZ ZA NAJWIĘKSZE ZAGROŻENIE DLA TWOICH DANYCH



KOMENTARZ FUNDACJI WTB

Dane gromadzone przez długie lata można stracić w ciągu jednej chwili. Może to spowodować działanie intencjonalne lub przypadek: kradzież, zgubienie urządzenia, uszkodzenie (np. dysku twardego), błąd ludzki (np. omyłkowe sformatowanie komputera albo „zresetowanie" go do ustawień fabrycznych, działanie wirusa, usunięcie niechcący danych i opróżnienie kosza), błąd oprogramowania (uszkodzenie systemu operacyjnego, uszkodzenie plików), wirus (np. ransomware szyfrujący dane i żądający zapłacenia okupu), hacker i wiele innych.

Ankietowani zostali zapytani o dwa rodzaje zagrożeń – utracenie danych oraz uzyskanie do nich dostępu przez osoby niepowołane. Ich odpowiedzi bazowały na subiektywnej ocenie prawdopodobieństwa - spojrzeli na te zagrożenia przez pryzmat własnych doświadczeń i wiedzy. Ryzyko wystąpienia tych niebezpieczeństw najlepiej dostrzegają właściciele firm, gdyż dane są im niezbędne do funkcjonowania biznesu, a ich kradzież może wpłynąć bezpośrednio na postrzeganie i konkurencyjność firmy.

OKIEM EKSPERTA

Zdecydowana większość zagrożeń dla bezpieczeństwa danych osobowych dotyczy danych przetwarzanych w systemach teleinformatycznych. Dzieje się tak dlatego, że systemy te ułatwiają gromadzenie i dokonywanie innych czynności przetwarzania danych na dużych zbiorach danych, często w sposób zautomatyzowany. Ponadto, systemy informatyczne służące do przetwarzania danych zazwyczaj umożliwiają dostęp za pośrednictwem sieci Internet – a brak odpowiednich zabezpieczeń może prowadzić np. do nieautoryzowanego dostępu do danych.

Zagrożeniem dla bezpieczeństwa danych jest jednakże nie tylko nieautoryzowany dostęp, spowodowany niewłaściwym zabezpieczeniem systemów służących do przetwarzania danych. Problemem jest także celowe działanie podmiotów, które świadcząc rozmaite usługi, przetwarzają dane niezgodnie z celem ich pozyskania, bez wiedzy i zgody osób, których dane dotyczą.

Kamila Kędzierska
Redaktor naczelna Informacja w administracji publicznej, Wydawnictwo C.H.Beck Sp. z o.o.
Radca prawny, pracownik aparatu administracji samorządowej

Jak traktujemy naruszenia prawa do ochrony danych osobowych?

Aż 42% respondentów twierdzi, iż w ich organizacjach nigdy nie doszło do naruszenia bezpieczeństwa danych.

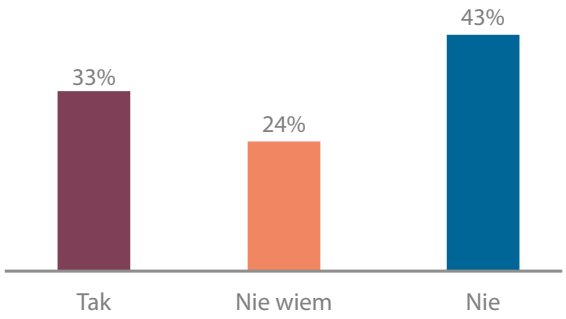
Jedna trzecia ogółu ankietowanych na pytanie czy kiedykolwiek naruszone zostało ich prawo do prywatności odpowiedziała twierdząco. Większość osób wskazała, że otrzymywała niechciane telefony z ofertami marketingowymi (83%) i niezamówione maile / spam (79%). Co ciekawe 70% badanych spotkało się z obiema wskazanymi formami wykorzystania danych bez ich zgody. Ponadto 9% respondentów zaznaczyło, że ich dane zostały opublikowane w Internecie, a 6%, że ktoś się pod nich podszył by zaciągnąć pożyczkę lub wziąć kredyt.

43% badanych uważa, że ich dane nie zostały nigdy wykorzystane bez ich zgody, a pozostali (24%) nie potrafili jednoznacznie wskazać odpowiedzi.

W podziale na grupy najwięcej odpowiedzi „tak, naruszone zostało moje prawo do prywatności" udzielili administratorzy bezpieczeństwa informacji (46%) oraz przedstawiciele kadry zarządzającej (44%). Twierdząco odpowiedziało też 30% pracowników i 26% osób nieaktywnych zawodowo.

We wszystkich badanych grupach najczęściej wskazywaną formą wykorzystania danych były telefony oraz maile z ofertami marketingowymi. Niechciane telefony otrzymało aż 94% ABI oraz przedstawicieli kadry zarządzającej, 81% pracowników oraz 61% niepracujących, niezamówione wiadomości zaś: 83% osób zajmujących się zawodowo ochroną danych osobowych, 82% managementu, 79% pracowników i 67% bezrobotnych lub uczących się.

CZY KIEDYKOLWIEK NARUSZONO TWOJE PRAWO DO OCHRONY DANYCH OSOBOWYCH?



› Zgłaszanie naruszeń

Tylko 35% respondentów, których naruszone zostało prawo do prywatności, zgłosiło takie zdarzenie do jakieś instytucji. Pozostałe osoby, w zróżnicowanych odpowiedziach wskazywały, dlaczego tego nie zrobiły. I tak: 35% respondentów zaznaczyło w ankiecie, że dochodzenie swoich praw wiązałoby się ze zbyt

OKIEM EKSPERTA

Co piąty respondent nie potrafił powiedzieć, czy jego prywatność została kiedykolwiek naruszona. Może to oznaczać niski poziom wiedzy o tym, czym jest ochrona danych osobowych, prawo do prywatności czy zagrożenia z tym związane. Edukacja w tym zakresie jest niezbędna, gdyż bez podstawowej wiedzy takie osoby mogą godzić się na wykorzystywanie ich danych osobowych w różnych celach, nie zdając sobie z tego sprawy.

Okazuje się, że znaczna część naruszeń ochrony danych osobowych, przynajmniej w odczuciu respondentów, dotyczy niechcianych przekazów marketingowych, czy to telefonicznych czy e-mailowych. Można zadać sobie pytanie, na ile są to rzeczywiste naruszenia – dane były wykorzystywane bezprawnie, np. bez zgody, a na ile respondenci nieświadomie lub bezrefleksyjnie wyrazili zgodę na wykorzystywanie ich danych przez administratorów danych lub ich partnerów w celach marketingowych. Warto też zastanowić się, czy tak mało wskazań na inne rodzaje naruszeń nie wynika z braku świadomości, że mają one miejsce. Może być przecież tak, że nie wiemy, że do wycieku naszych danych doszło tak długo, jak nie zostaną one bezprawnie wykorzystane np. w celu zaciągnięcia pożyczki. Zmianę może tu przynieść ogólne rozporządzenie o ochronie danych, które w niektórych przypadkach będzie zobowiązywało administratorów do informowania klientów o naruszeniach ich danych osobowych.

Nie dziwi natomiast, że najwięcej osób spośród administratorów bezpieczeństwa informacji stwierdziło, że ich prawo do prywatności zostało naruszone. Są to osoby, dla których ochrona danych osobowych jest codziennością, mają więc dużą świadomość, także tego, kiedy ich dane są niewłaściwie wykorzystywane.

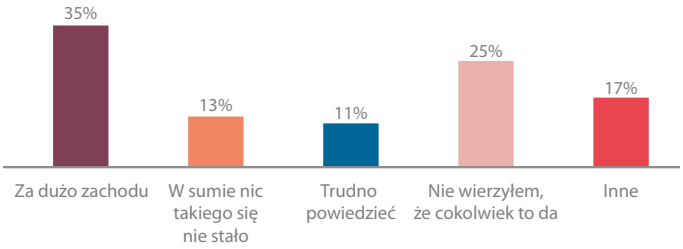
Wioleta Szczygielska
Redaktor prowadząca miesięczników „Ochrona danych osobowych", „Dokumentacja ODO" i portalu PoradyODO.pl, Wydawnictwo Wiedza i Praktyka sp. z o.o.

dużym zachodem, 25% stwierdziło, że zgłoszenie nie wiele by dało, 13% uznało, że „nic takiego się nie stało", 17% zaznaczyło, odpowiedź „inne", a 11% nie potrafiło jednoznacznie odpowiedzieć, jaki był powód ich bierności.

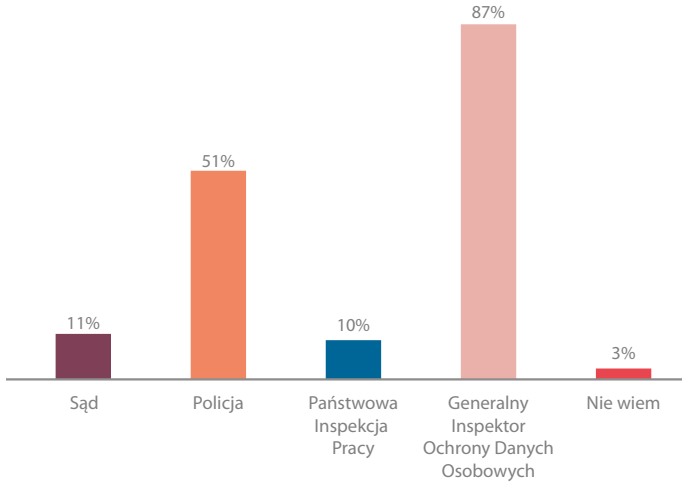
Największy odsetek ankietowanych, którzy nie zgłosili naruszenia ochrony danych osobowych zanotowaliśmy w grupie obejmującej osoby nieaktywne zawodowo (78%). Na drugim miejscu znalazła się kadra zarządzająca (71%), na trzecim pracownicy (62%), a na ostatnim specjaliści z zakresu ochrony danych osobowych (61%). We wszystkich badanych grupach dominującym powodem niezgłaszania naruszeń ochrony danych osobowych było przekonanie, że nie jest to warte poświęcenia ich czasu i nie przyniesie pożądanego rezultatu. Znaczna cześć ankietowanych jest także przeświadczona o tym, że są to czyny o niskiej szkodliwości.

Uczestnicy badania zapytani o to, do kogo można zgłaszać incydenty z zakresu danych osobowych odpowiadali, że do: Generalnego Inspektora Ochrony Danych Osobowych – 87%, policji – 51%, sądu – 11% i Państwowej Inspekcji Pracy – 10%. 3% respondentów nie wskazało żadnego z wymienionych podmiotów.

POWODY NIE ZGŁASZANIA NARUSZEŃ



GDZIE MOŻNA ZGŁOSIĆ NARUSZENIE OCHRONY DANYCH



OKIEM EKSPERTA

Skargi na przetwarzanie danych osobowych należy składać do Generalnego Inspektora Ochrony Danych Osobowych i/lub na policję. Ważne jest to by procedury zgłaszania naruszeń ochrony danych osobowych były wdrożone w organizacjach, Jest to jeden z elementów zapewnienia zgodnego z prawem przetwarzania danych osobowych. Nie zgłaszanie incydentów wpływa na to, że podmioty naruszające prywatność mogą czuć się bezkarne.

W największym stopniu na uwagę zasługują dwie pierwsze odpowiedzi wskazujące na przyczyny braku zgłoszeń incydentów, a więc te, które zaznaczyła największa liczba respondentów. Dają one wyraz aktualnej sytuacji związanej z postrzeganiem zarówno samych urzędów dedykowanych do zajmowania się ochroną danych osobowych i niezgodnym z prawem ich wykorzystaniem jak i ich sposobami działania. Mianowicie niewydolność przedmiotowych instytucji, a często także brak faktycznego zainteresowania naruszeniami z tego zakresu i traktowanie spraw dotyczących prywatności jako spraw mniejszej wagi jest zasadniczą przyczyną obecnego stanu rzeczy.

Dodatkowo należy zwrócić uwagę, iż najwięcej respondentów wskazało, że zgłoszenie jak i sam proces dochodzenia swoich praw jest nadmiernie utrudniony i wymaga zbyt dużego zaangażowania ze strony osób zgłaszających. Z moich prywatnych doświadczeń wynika nie tylko brak zainteresowania ze strony podmiotów dedykowanych, lecz także towarzyszy mi nieodparte poczucie, że wręcz podejmują one starania, aby sprawy „odepchnąć" i w ogóle, w miarę możliwości, się nimi nie zajmować. Wszystkie te elementy składają się właśnie na wyrażone przez respondentów opinie, których nie można uznać za bezpodstawne.

Aleksandra Piotrowska
Prezes zarządu, Fundacja Wiedza To Bezpieczeństwo

› Incydenty w organizacjach

Ankietowani aktywni zawodowo zostali zapytani także o to, czy w ich firmach zdarzały się incydenty naruszenia bezpieczeństwa danych, takie jak np. kradzież laptopa lub smartfonu, udostępnienie danych osobom nieupoważnionym lub wysłanie maila zawierającego dane osobowe do niewłaściwego adresata. Aż 26% osób stwierdziło, że takie zdarzenie miało miejsce, w tym 7% wskazało, że stało się to nawet kilkukrotnie. 42% respondentów odpowiedziało, że w organizacjach, z którymi są związani, incydenty związane z ochroną danych osobowych nigdy się nie zdarzyły, a 32% wskazało, że nie wie o takich sytuacjach. Co ciekawe aż 68% osób, które zarządzają firmami stwierdziło, że nie odnotowano w nich żadnych naruszeń.

Najmniejszą wiedzę o incydentach mają pracownicy – 40% z nich nie odpowiedziało ani twierdząco, ani przecząco na to pytanie.

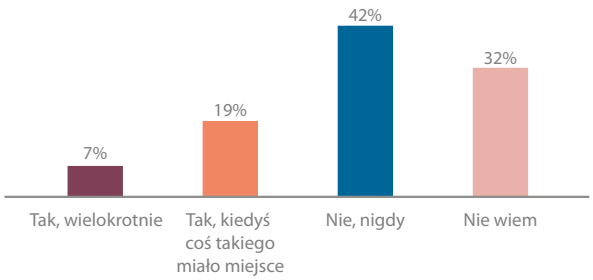
Ponadto osoby, które wskazały, że w ich organizacjach miały miejsce incydenty zapytane zostały o to, po jakim czasie zostały one zgłoszone. Zdecydowana większość (64%) odpowiedziała, że stało się to w ciągu 24 godzin. Pozostali zaznaczyli, że było to 48 godzin (16%), 72 godziny (9%) lub inny okres (10%). Ponadto warto dodać, że 88% respondentów stwierdziło, że wie komu należy zgłosić naruszenie bezpieczeństwa danych osobowych w swojej organizacji.

OKIEM EKSPERTA

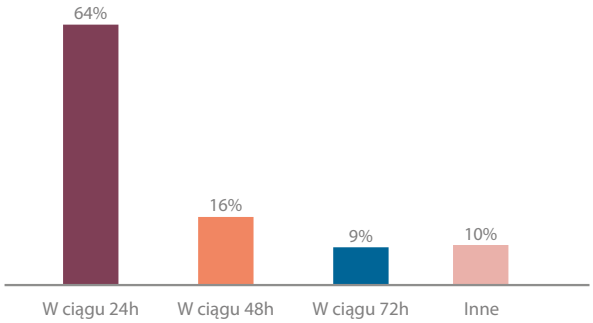
Incydenty bezpieczeństwa informacji w organizacjach są rzeczą naturalną. Zdarzają się niemal w każdej firmie i trudno dziś wyobrazić sobie organizację, w której nigdy nikt nie dowiedział się o czymś, o czym nie powinien, bądź też gdzie nie wystąpiła nigdy awaria skutkująca brakiem dostępu do pewnych informacji. Zastanawiające jest więc dlaczego aż 42% respondentów twierdzi, iż w ich organizacjach incydenty nigdy się nie wydarzyły. Należy przypuszczać, że w takich organizacjach nie ma zdefiniowanej ścieżki obsługi incydentów bezpieczeństwa informacji bądź też wiedza na temat tego, czym są incydenty bezpieczeństwa informacji wśród pracowników jest niewielka. W każdej organizacji warto rozważyć wdrożenie procedur związanych z zarządzaniem tymi incydentami. Aby nie wyważać otwartych drzwi najwygodniej zastosować zasady opisane w międzynarodowym standardzie ISO/IEC 27001:2013. Procedury związane z zarządzaniem incydentami powinny uwzględniać elementy związane z zakresem odpowiedzialności, opisem kanałów służących zgłaszaniu informacji o potencjalnych incydentach przez pracowników, oceną i klasyfikacją incydentu, zautomatyzowaniem reakcji na incydent, wyciąganiu wniosków z tego co już się wydarzyło aby zminimalizować ryzyko wystąpienia podobnego zdarzenia w przyszłości, a jeśli incydent ma mieć finał w sądzie, prawidłowo przygotować elektroniczny dowód sądowy. Po opracowaniu odpowiednich procedur każdy z pracowników powinien być z nimi zapoznany i mógł skutecznie zareagować w przypadku wystąpienia incydentu. Aby zminimalizować ryzyko jego wystąpienia konieczne są szkolenia pracowników w zakresie aktualnych zagrożeń tak aby to PRACOWNIK BYŁ NAJMOCNIEJSZYM ogniwem sytemu zarządzania bezpieczeństwem informacji w organizacji.

Przemysław Szczurek
Product Manager ds. bezpieczeństwa informacji, TUV NORD Polska sp. z o.o.

CZY W TWOJEJ FIRMIE ZDARZAŁY SIĘ INCYDENTY NARUSZENIA BEZPIECZEŃSTWA OCHRONY DANYCH



W JAKIM CZASIE ZAISTNIAŁY INCYDENT ZOSTAŁ ZGŁOSZONY



RODO coraz bliżej. Czy widać to w organizacjach?

Ponad połowa aktywnych zawodowo odpowiada twierdząco. 26% badanych twierdzi, że zmiany nie zostały jeszcze wprowadzone, a 23% nie ma wiedzy na ten temat.

25 maja 2018 roku zacznie obowiązywać europejskie rozporządzenie o ochronie danych osobowych (RODO). Unia Europejska przewidziała dwuletni okres dostosowawczy na wdrożenie nowych regulacji. Zapytaliśmy pracowników, kadrę zarządzającą i ABI o stan przygotowań do wdrożenia nowych przepisów w podmiotach, z którymi są związani. W pierwszej kolejności zadaliśmy pytanie, czy w ich organizacjach wprowadzono już zmiany w procedurach przetwarzania danych osobowych, w związku ze zmianą przepisów o ochronie danych osobowych (RODO). Odpowiedziała na nie twierdząco ponad połowa (51%) respondentów. Warto zauważyć, że jest to wynik odzwierciedlający wskazania we wszystkich grupach, wariant „tak" wybrało bowiem 51% pracowników, 54% kadry zarządzającej i 49% ABI. 26% badanych stwierdziło, że zmiany nie zostały jeszcze wprowadzone, a 23% nie miała wiedzy na ten temat. Co ciekawe tylko specjaliści z zakresu ochrony danych osobowych potrafili jednoznacznie wybrać między odpowiedziami „tak" i „nie" (1% odpowiedzi „nie wiem"). 27% ankietowanych stwierdziło, że zostało raz wprowadzonych w nowe obowiązki w zakresie przetwarzania danych osobowych, a aż 41%, że stało się to kilkukrotnie.

Zgodnie z RODO dotychczasowego ABI odpowiedzialnego za zgodne z prawem przetwarzanie danych w organizacji, zastąpi Inspektor Ochrony Danych. Postanowiliśmy jednak zapytać uczestników badania, czy w ich organizacjach planowane jest jego powołanie. 48% osób odpowiedziało twierdząco na tak zadane pytanie, a 40% nie potrafiło na nie odpowiedzieć. 76% ABI i 54% kadry zarządzającej stwierdziło, że w ich organizacjach zostanie powołany IOD.

› *Wiedza i potrzeba szkoleń*

Aż 88% ankietowanych deklaruje znajomość nowych przepisów o ochronie danych osobowych, ale jedynie co piąty z nich uznaje, że jego wiedza jest w pełni wystarczająca. Pozostali chętnie dowiedzieliby się czegoś więcej. Potrzebę uczestniczenia w szkoleniu i poszerzenia wiedzy z obszaru ochrony danych osobowych odczuwa aż 68% ankietowanych.
W grupie specjalistów z zakresu ochrony danych osobowych jest to 100%, podczas gdy wśród managementu jest to 67%, a pracowników 63%. Tylko co 10 osoba biorąca udział w badaniu wskazała, że nie czuje potrzeby pogłębiania swojej wiedzy poprzez szkolenie. Pozostali (23%) ankietowani nie byli pewni, czy chcieliby wziąć udział w szkoleniu z zakresu ochrony danych osobowych.

OKIEM EKSPERTA

Do maja 2018 r. – kiedy zacznie obowiązywać RODO - pozostało niewiele czasu. Tymczasem 26% ankietowanych deklaruje, że w ich organizacji nie wprowadzono jeszcze żadnych zmian w procedurach przetwarzania danych osobowych. Dalsze 23% nie ma na ten temat wiedzy.

Bardzo dobrym znakiem jest wysoka chęć poszerzania swojej wiedzy wśród specjalistów, są oni świadomi tego, że jeśli nie będą na bieżąco edukowani, nie będą mogli skutecznie wykonywać swoich obowiązków. Natomiast 1/3 kadry kierowniczej, która powinna doskonale wiedzieć czym jest RODO nie czuje w ogóle żadnej potrzeby edukacji w tym zakresie – a to nie jest najlepszy sygnał. Można podejrzewać, że w takich organizacjach zakłada się, że nowe przepisy wdroży dział informatyki albo prawny i prawie, że na pewno będzie skutkowało to tym, że takie firmy nie będą przygotowane do nowych przepisów.

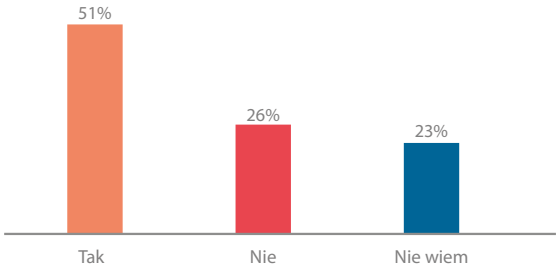
Szkolenia są podstawą systemu ochrony danych osobowych, tym czasem aż co trzeci pracodawca przyznaje, że jego pracownicy takich szkoleń nigdy nie mieli. Trudno sobie wyobrazić, aby ochrona danych, zarówno dzisiaj jak i w przyszłości - funkcjonowała sprawnie bez szkoleń. Pamiętajmy, RODO wprowadza bardzo wysokie kary, a bez szkoleń, edukacji i budowania świadomości o naruszenia będzie łatwo.

Wyniki ankiety pokazują, że wśród kadry innej niż specjaliści od ochrony danych osobowych trzeba budować potrzebę rozwijania wiedzy, która pozwoli bezpiecznie przetwarzać dane i zarządzać systemem ochrony danych osobowych.

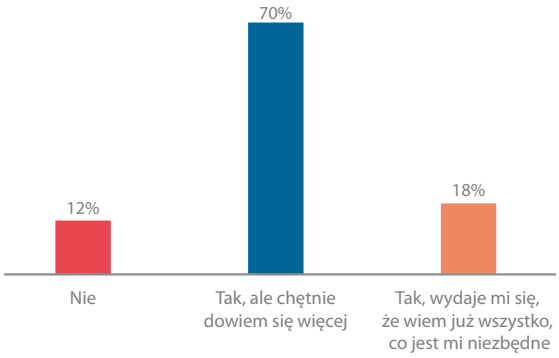
Leszek Kępa
Wiceprzewodniczący Rady, Fundacja Wiedza To Bezpieczeństwo

41% przedsiębiorców twierdzi, że ich pracownicy zostali kilkukrotnie przeszkoleni z zakresu ochrony danych osobowych, a 31%, że miało to miejsce jeden raz. Niestety 28% przyznaje, że nigdy nie przeszkoliło swoich podwładnych. Jeśli chodzi o częstotliwość szkoleń to w prawie połowie (47%) organizacji odbywają się one rzadziej niż raz w roku, raz w roku organizuje je 28%, a częściej 28%.

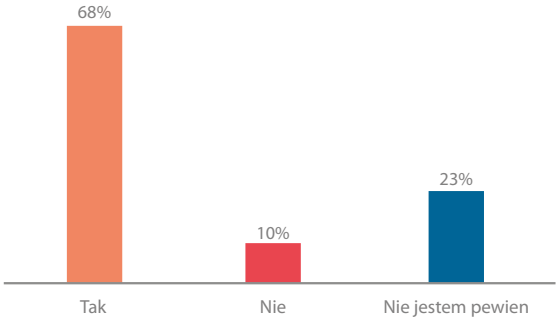
CZY W TWOJEJ ORGANIZACJI TRWAJĄ PRZYGOTOWANIA DO RODO



CZY MASZ WYSTARCZAJĄCĄ WIEDZĘ NA TEMAT NOWYCH PRZEPISÓW



CZY ODCZUWASZ POTRZEBĘ UCZESTNICZENIA W SZKOLENIU Z OCHRONY DANYCH OSOBOWYCH



› *Ochrona danych osobowych w organizacjach okiem kadry zarządzającej*

Przedsiębiorców i osoby zarządzające firmami zapytaliśmy, czy wiedzą, jakie obowiązki na organizacje nakłada unijne rozporządzenie o ochronie danych. Twierdząco odpowiedziało zaledwie 55% osób. Zaledwie połowa respondentów przeprowadza w swojej organizacji szacowanie ryzyka przy przetwarzaniu danych osobowych. Jest ono jednym z najważniejszych elementów odpowiedniego dostosowania procedur nakładanych przez przepisy RODO.

Podobnie jak obecnie, przedsiębiorcy na gruncie nowych przepisów będą pełnić funkcje administratora danych osobowych (ADO). Prawie jedna trzecia (31%) respondentów stwierdziła, że wie, jakie będą ich obowiązki związane z ochroną danych w organizacji po 25 maja 2018 roku.

OKIEM EKSPERTA

Połowa organizacji wie, jak trzeba przygotować się do nowych przepisów, ale być może nie najlepiej komunikuje to osobom zajmującym się obecnie ochroną danych osobowych. Jak pokazało badanie, nie wiedzą oni jeszcze, jakie będą ich obowiązki po 25 maja 2018 r. Przekształcenie systemu ochrony danych osobowych z regulowanego przepisami prawa w system regulowany samodzielnie na podstawie przeprowadzonej analizy ryzyka, jest elementem obcym dla większości badanych organizacji. Od strony praktycznej, znacznie łatwiej jest administratorom danych dostosować się do wytycznych organu nadzorczego, nie zastanawiając się nad adekwatnością stosowanych zabezpieczeń danych osobowych. Dodatkowym elementem utrudniającym cały proces dostosowawczy jest wymóg uwzględniania ochrony danych osobowych w fazie projektowania produktu lub usługi. Jest to bowiem całkowite odwrócenie sytuacji. Obecnie badanie zgodności z przepisami prawa nowego procesu w organizacji, odbywa się najczęściej już po jego wdrożeniu. Podsumowując, organizacje czytając literalnie przepisy RODO, próbują je interpretować na swoją korzyść. Nie dostrzegają przy tym zmiany całej koncepcji ochrony danych osobowych w UE. Pierwsze kontrole nowego organu nadzorczego pokażą w praktyce, jak duże zmiany powinny były nastąpić w organizacji. Wtedy część spóźnionych przedsiębiorców rozpocznie wyścig z czasem, którego lepiej uniknąć wdrażając nowe regulacje już dziś.

Konrad Gałaj – Emiljańczyk
Ekspert ds. ochrony danych, ODO 24 sp. z o. o.

Ankietowanych zapytaliśmy także o to, czy ich organizacja będzie zobowiązana do wyznaczenia IOD. Odpowiedzi były bardzo zróżnicowane – „tak" odpowiedziało 25%, „nie" – niecałe 38%, a pozostali nie wiedzieli, czy są zobligowani do jego powołania.

› *Administratorzy bezpieczeństwa informacji a RODO*

75% osób zajmujących się ochroną danych osobowych lub ochroną informacji przyznaje, że nie jest to ich jedyna funkcja w organizacjach. Często muszą godzić ją np. z obowiązkami informatyka lub prawnika. Zgodnie z nowymi regulacjami ABI zastąpi IOD. Jest to nie tylko zmiana nazwy, ale także obowiązków, które trudno będzie pogodzić z innymi zadaniami w organizacji.

Większość ABI (52%) twierdzi, że posiada wystarczającą wiedzę, aby pełnić funkcję IOD. Pozostała część stara się samodzielnie lub korzystając ze specjalistycznych szkoleń zwiększyć swoje kompetencje w zakresie ochrony danych osobowych. 54% respondentów z tej grupy stwierdziło, że zna szczegółowo zakres zmian, jakie wprowadza RODO, a 46% posiada ogólną wiedzę, którą chciałoby pogłębić.

Zapytaliśmy specjalistów z zakresu ochrony danych osobowych także o to, kiedy ich organizacje planują dostosowanie procesów przetwarzania danych do wymogów unijnego rozporządzenia o ochronie danych. Zdecydowana większość (67%) stwierdziła, że do 25 maja 2018 roku – dnia, w którym zaczną obowiązywać nowe regulacje.

Obecnie ABI podlega zarządowi lub kierownictwu firmy i 93% grupy jest zdania, że się to nie zmieni.

Tylko 34% ABI uważa, że świadomość najwyższego kierownictwa firmy, w której pracują, w zakresie wymagań, jakie stawia unijne rozporządzenie o ochronie danych, jest wysoka (22%) lub bardzo wysoka (12%). Czterech na dziesięciu (39%) badanych uważa, że świadomość jest na średnim poziomie, a pozostali, że niskim lub bardzo niskim.

Europejskie rozporządzenie o ochronie danych osobowych znacznie rozszerza zakres obowiązków inspektora ochrony danych w stosunku do obecnego ABI. Ponad połowa ABI jest przygotowana na „transformację" swoich obowiązków. Możliwe, że słaby postęp przygotowań do RODO wynika z nie dość – zdaniem ABI - wysokiej świadomości kadry kierowniczej, chociaż – co ciekawe - sama kadra kierownicza uważa, że wymagania stawiane przez RODO zna wystarczająco.

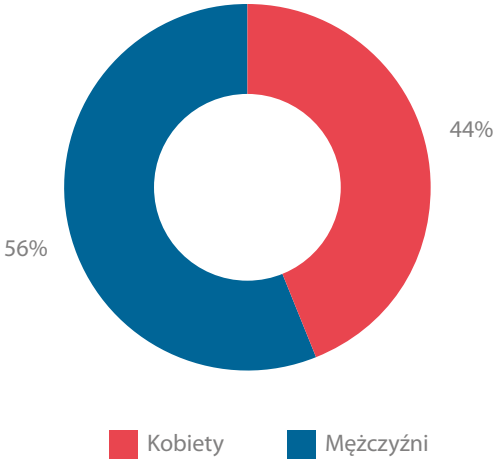
OKIEM EKSPERTA

Obszar ochrony danych w przedsiębiorstwach jest krytycznym elementem dla wielu spółek oraz organizacji sektora publicznego. Osoby zajmujące stanowiska ABI, jak również i w kolejnym kroku IOD, powinny w pełni (bez angażowania się w inne zadania) poświęcić powierzonym zadaniom. Część z organizacji może sobie pozwolić na pełnoetatowe stanowiska wewnątrz własnych struktur (dotyczy to zazwyczaj dużych przedsiębiorstw), a część ma możliwość skorzystania z zewnętrznego wsparcia. Już obecnie w modelu outsourcingowym kwestiami ochrony danych zajmują się np. firmy consultingowe, kancelarie prawne oraz specjalistyczne organizacje, dla których administracja bezpieczeństwem informacji, czy też ochrona danych stanowi główny obszar działalności. Podobnie jak ma to miejsce w innych obszarach, gdzie outsourcing ma swoje zastosowanie, ochrona danych wymaga specjalistycznej wiedzy, doświadczenia czy też dostosowywania się do europejskich i polskich przepisów prawa. Nowe przepisy, które zaczną w pełni obowiązywać od maja 2018 dają przedsiębiorcom jeszcze około roku czasu na poczynienie niezbędnych kroków, aby we właściwy sposób zadbać o uruchomienie stanowisk IOD lub skorzystanie z oferty outsourcingowej tych usług. Jak to bywa z wprowadzaniem unijnych i krajowych rozporządzeń, termin 12 miesięcy to raczej krótki okres i przedsiębiorstwa już teraz powinny, bez dalszych opóźnień, skupić się na realizacji wymogów, które dotyczą ochrony danych. Do czasu obowiązywania nowych regulacji, wymagania stawiane przez RODO powinny być znacznie mocniej nagłaśniane (zarówno przez regulatora, odpowiednie Ministerstwo oraz media biznesowe), a świadomość kadry kierowniczej, jak i samych ABI powinna być rozwijana tak, aby we właściwy i zgodny z prawem sposób, zaadaptować nowe przepisy.

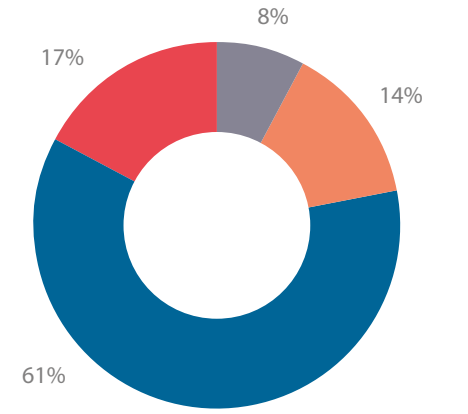
Wiktor Doktór
Prezes, Pro Progressio

Charakterystyka uczestników badania

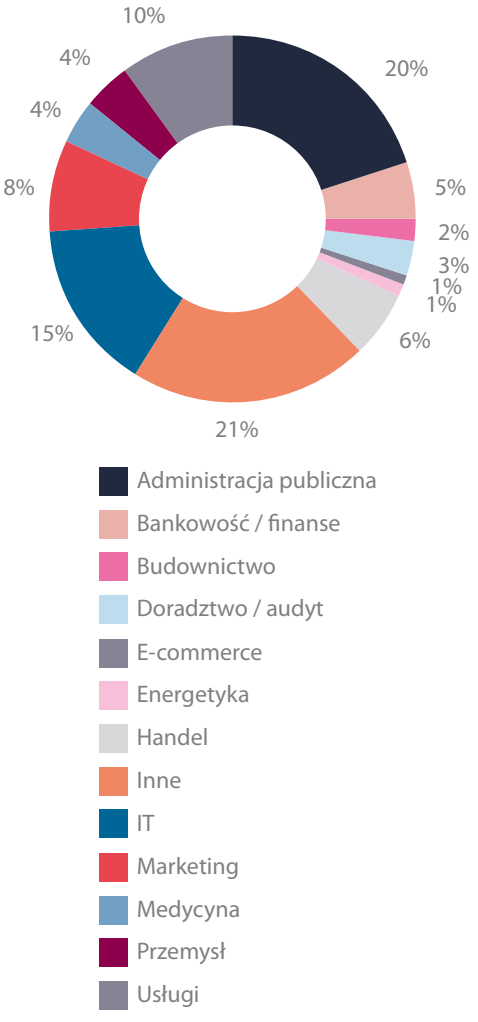
PŁEĆ



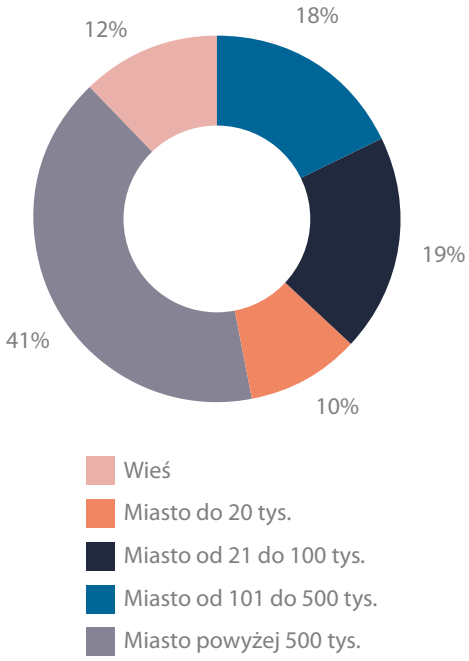
SYTUACJA ZAWODOWA



OBSZAR ZATRUDNIENIA



MIEJSCE ZAMIESZKANIA



› Notatki

FUNDACJA
WIEDZA TO BEZPIECZEŃSTWO

PODSTAWOWE ZASADY OCHRONY

- Traktuj dane osobowe innych tak, jak chciałbyś, by były traktowane Twoje.
- Po zakończeniu pracy, chowaj dane osobowe z zasięgu wzroku i dłoni osób niepowołanych.
- 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.
- Pracując na danych osobowych, korzystaj tylko z sieci zabezpieczonych hasłem.
- Nie wyrzucaj dokumentów zawierających dane osobowe do śmietnika – korzystaj z niszczarek.
- Nie pozostawiaj osób nieupoważnionych z danymi osobowymi bez nadzoru.
- Zmieniaj swoje hasła dostępowe, nikomu ich nie przekazuj i nie zapisuj w widocznych miejscach

PARTNERZY BADANIA

ODO24 · C.H.BECK · Wiedza i Praktyka · PROPROGRESSIO · TÜV NORD · Wolters Kluwer Polska · callcenter forum.pl

PATRONI MEDIALNI

informacja w administracji publicznej · OCHRONA DANYCH OSOBOWYCH · outsourcing portal · OutsourcingMore · Fundacja nowoczesna Polska · KLIENTMANIA