Zasady ochrony informacji oraz organizacji przetwarzania i ochrony danych osobowych w Poczcie Polskiej S.A.

Zmiany w wewnętrznych aktach prawnych, przypomnienie o zasadach ochrony informacji

- Zmiany w Polityce bezpieczeństwa przetwarzania danych osobowych oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Poczcie Polskiej S.A. m.in. w związku ze zmianami w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz przepisach wydanych na jej podstawie.
- Polityka bezpieczeństwa informacji w Poczcie Polskiej S.A.

Informacje prawnie chronione

To informacje stanowiące m.in. tajemnicę:

- ✔ przedsiębiorstwa,
- ✔ pocztową,
- ✔ bankową,
- ✔ ubezpieczeniową,
- ✔ dane osobowe

zgodnie z definicjami zawartymi w odpowiednich przepisach prawa powszechnie obowiązującego (ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, ustawa z dnia 23 listopada 2012 r. Prawo pocztowe, ustawa z dnia 28 sierpnia 1997 r. Prawo bankowe, ustawa z dnia 22 maja 2003 r. o działalności ubezpieczeniowej, ustawa z dnia 22 maja 2003 r. o pośrednictwie ubezpieczeniowym, ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych).

Niniejsza prezentacja nie dotyczy ochrony informacji niejawnych w rozumieniu ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych

Co oznacza bezpieczeństwo informacji?

Bezpieczeństwo informacji to zachowanie właściwego poziomu (adekwatnego do podatności i ryzyk, wynikających m.in. z rodzaju informacji podlegających ochronie):

- ✔poufności (informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom),
- ✔integralności (informacja ma być dokładna i kompletna),
- ✔dostępności (informacja ma być dostępna i użyteczna na żądanie upoważnionego podmiotu),

a w uzasadnionych przypadkach dodatkowo:

- ✔rozliczalności (działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi),
- ✔niezaprzeczalności (umożliwienia rozstrzyganie wszelkich sporów dotyczących wystąpienia lub niewystąpienia deklarowanego zdarzenia lub działania),
- ✔autentyczności (tożsamość podmiotu lub zasobu jest taka, jak deklarowana),
- ✔niezawodności (oznacza spójne, zamierzone zachowanie i skutki).

Zasady dostępu do informacji prawnie chronionych

- **Pracownik Spółki**: jest uprawniony do korzystania z informacji prawnie chronionych wyłącznie w zakresie niezbędnym do wykonywania obowiązków służbowych lub przedsięwzięć biznesowych (zasada wiedzy uzasadnionej). Prawo dostępu do określonego aktywu informacyjnego ma charakter indywidualny, jest przypisane do konkretnej osoby i zostaje odebrane w momencie zmiany zakresu obowiązków służbowych (ew. zmodyfikowane) lub ustania stosunku pracy. Uzyskanie uprawnienia dostępu do aktywów informacyjnych poprzedza instruktaż w zakresie ochrony informacji i odpowiedzialności za jej naruszenie oraz podpisanie oświadczenia zobowiązującego do realizacji wymagań bezpieczeństwa informacji.
- **Podmiot zewnętrzny**: jest uprawniony do korzystania z informacji prawnie chronionych w zakresie niezbędnym do realizacji umów cywilnoprawnych (po wprowadzeniu niezbędnych zabezpieczeń oraz po podpisaniu umowy określającej wymagania bezpieczeństwa) albo w przypadkach przewidzianych przepisami prawa. Dostęp do informacji oraz środków ich przetwarzania odbywa się pod kontrolą, sprawowaną przez gestora informacji.

Odpowiedzialność, zgłaszanie incydentów

Osoby, uzyskujące dostęp do informacji są zobowiązane do **przestrzegania wymagań bezpieczeństwa informacji i bezpieczeństwa informatycznego**, w szczególności w zakresie ochrony danych osobowych, tajemnicy pocztowej, bankowej i innych tajemnic prawnie chronionych oraz **bezwzględnego zgłaszania każdego incydentu bezpieczeństwa (w tym zagrożenia takim incydentem**) bezpośredniemu przełożonemu tak szybko, jak jest to możliwe. Szczegółowe wymagania w zakresie obiegu informacji o incydentach bezpieczeństwa informatycznego określają odrębne wewnętrzne akty prawne.

W przypadku naruszenia wymagań bezpieczeństwa informacji i bezpieczeństwa informatycznego **osoba winna naruszenia podlega odpowiedzialności określonej we właściwych przepisach, w tym odpowiedzialności porządkowej oraz materialnej.**

Czym jest tajemnica przedsiębiorstwa?

Tajemnicę przedsiębiorstwa stanowią nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności (art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji).

Określone informacje spełniają kryteria niezbędne do uznania ich za tajemnicę przedsiębiorstwa **o ile wyczerpują wszystkie trzy przesłanki**, tj.:

- ✔są ściśle związane z prowadzoną przez Pocztę Polską S.A. działalnością gospodarczą i mają dla Spółki bezsprzecznie wartość gospodarczą (wartość gospodarcza może wyrażać się zarówno w interesie stricte majątkowym, np. zestawienie kontrahentów, polityka cenowa wobec klientów biznesowych, jak i niemajątkowym, np. informacje mogące wpłynąć na renomę Spółki),
- ✔informacje te nie zostały ujawnione do wiadomości publicznej (w szczególności są nieznane ogółowi lub osobom, które ze względu na wykonywany zawód są zainteresowane jej posiadaniem, nie można dowiedzieć się o nich drogą zwyczajową),
- ✔Poczta Polska S.A. podjęła w stosunku do nich niezbędne działania w celu zachowania ich poufności (tj. wyraża łatwo dostrzegalną wolę, aby dana informacja pozostała tajemnicą, podejmowane są działania, które zgodnie z wiedzą i doświadczeniem życiowym powinny zapewnić ochronę informacji przed jej upublicznieniem, jak i zabezpieczające wgląd do tych informacji).

Klasyfikacja informacji stanowiących tajemnicę przedsiębiorstwa

Za wskazywanie informacji podlegających ochronie i określanie zakresu tej ochrony odpowiada gestor informacji, tj. kierownik struktury/jednostki/samodzielnej komórki organizacyjnej, odpowiadający za realizację zadań Spółki, z którymi wiąże się przetwarzanie określonego zakresu aktywów informacyjnych lub których realizację wspiera dany system informatyczny.

Uprawniony odbiorca informacji podlegających ochronie winien zostać poinformowany, że udostępniona informacja podlega ochronie. W przypadku informacji zawartych np. w korespondencji - poprzez opatrzenie ich klauzulą „tajemnica przedsiębiorstwa Poczta Polska S.A." (w prawym górnym rogu – w przypadku, gdy cała treść dokumentu stanowi tajemnicę przedsiębiorstwa, zaś w przypadku, gdy tajemnicę stanowi wybrana informacja – należy ją wyraźnie wskazać w treści pisma, np. „Tajemnicą przedsiębiorstwa objęto: podać zakres informacji"). W uzasadnionych przypadkach należy wskazać uzasadnienie objęcia ochroną określonej informacji – zgodnie z definicją tajemnicy przedsiębiorstwa.

Możliwe jest również określenie daty lub wydarzenia, po którym wskazana informacja przestaje być objęta ochroną, np. „Okres ochrony przedmiotowej informacji upływa po opublikowaniu sprawozdania finansowego Poczty Polskiej S.A. za rok obrotowy *podać rok*".

Zakres informacji objętych ochroną może być określony również w umowie, będącej podstawą udostępnienia informacji stanowiących tajemnicę przedsiębiorstwa.

Czym jest tajemnica pocztowa?

Tajemnica pocztowa obejmuje informacje przekazywane w przesyłkach pocztowych, informacje dotyczące realizowania przekazów pocztowych, dane dotyczące podmiotów korzystających z usług pocztowych oraz dane dotyczące faktu i okoliczności świadczenia usług pocztowych lub korzystania z tych usług.

Do zachowania tajemnicy pocztowej są obowiązany jest operator pocztowy i osoby, które z racji wykonywanej działalności mają dostęp do tajemnicy pocztowej. Obowiązek zachowania tajemnicy pocztowej jest nieograniczony w czasie.

Naruszeniem obowiązku zachowania tajemnicy pocztowej jest w szczególności:

1) ujawnianie lub przetwarzanie informacji albo danych objętych tajemnicą pocztową;

2) otwieranie zamkniętych przesyłek pocztowych lub zapoznawanie się z ich treścią;

3) umożliwianie osobom nieuprawnionym podejmowania działań mających na celu wykonywanie czynności, o których mowa w pkt 1 i 2.

Informacje lub dane objęte tajemnicą pocztową mogą być zbierane, utrwalane, przechowywane, opracowywane, zmieniane, usuwane lub udostępniane tylko wówczas, gdy czynności te dotyczą świadczonej usługi pocztowej albo są niezbędne do jej wykonania lub jeżeli przepisy odrębne stanowią inaczej.

Jakie informacje stanowią dane osobowe?

Za **dane osobowe** uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (tj. takiej, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo specyficzne czynniki, określające jej cechy fizyczne, fizjologiczne umysłowe, ekonomiczne, kulturowe lub społeczne).

Dane osobowe mogą przybrać różną formę – to także wizerunek (zdjęcie, film), zarejestrowany głos, dane biometryczne (linie papilarne), adres IP, adres e-mail.

Dane osobowe można zaliczyć do dwóch kategorii:

- tzw. dane sensytywne (wrażliwe) – czyli ujawniające pochodzenie rasowe, etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, dane o stanie zdrowia, kodzie genetycznym, nałogach, życiu seksualnym, danych dotyczących skazań, orzeczeń o ukaraniu, mandatów karnych a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym,
- tzw. dane zwykłe – wszystkie dane osobowe, które nie zostały uznane za wrażliwe.

Przetwarzanie danych osobowych

To jakiekolwiek operacje na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

Każdy z podmiotów, uczestniczących w procesie przetwarzania danych (z wyjątkiem osoby, której dane dotyczą) może być kwalifikowany jako:

- ✔administrator danych osobowych (tj. organ, jednostka organizacyjna, podmiot lub osoba, która decyduje o celach i środkach przetwarzania danych osobowych). Status administratora danych osobowych, przetwarzanych w zbiorach danych Poczty Polskiej S.A., w tym pracowników Spółki, posiada Poczta Polska S.A. z siedzibą przy ul. Rodziny Hiszpańskich 8 w Warszawie.
- ✔podmiot, któremu administrator danych powierzył przetwarzanie danych w drodze umowy zawartej na piśmie (tzw. procesor, który może przetwarzać dane osobowe wyłącznie w celu i zakresie przewidzianym w umowie. Poczta Polska S.A. przetwarza na tej podstawie np. dane osobowe klientów Banku Pocztowego S.A.).

Inne podmioty, związane z przetwarzaniem danych, działają w imieniu jednego z ww. podmiotów - np. osoba upoważniona do przetwarzania danych.

Zasady przetwarzania danych osobowych (1)

Przesłanki dopuszczalności przetwarzania danych osobowych tzw. zwykłych:

- ✔**zgoda** osoby, której dane dotyczą (np. zgoda osoby, której dane dotyczą, na marketing produktów i usług bankowych/ubezpieczeniowych drogą elektroniczną),
- ✔jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego **z przepisu prawa** (np. dane klientów przetwarzane na w celu i zakresie określonym w ustawie z dnia 23 listopada 2012 r. Prawo pocztowe, dane pracowników – w celu i zakresie określonym w ustawie z dnia 26 czerwca 1974 r. Kodeks pracy),
- ✔jest to konieczne **do realizacji umowy**, **gdy osoba, której dane dotyczą jest jej stroną** lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
- ✔jest to niezbędne do wykonania **określonych prawem** zadań realizowanych **dla dobra publicznego,**
- ✔jest to niezbędne dla wypełnienia **prawnie usprawiedliwionych celów** realizowanych przez administratorów danych albo odbiorców danych a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. Za prawnie usprawiedliwiony cel uważa się w szczególności marketing bezpośredni własnych produktów i usług administratora danych i dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej.

Zasady przetwarzania danych osobowych (2)

Art. 27 ust. 1 ustawy o ochronie danych osobowych ustanawia generalny zakaz przetwarzania danych osobowych tzw. sensytywnych chyba, że zachodzą okoliczności wskazane w ust. 2, tj. **w szczególności**:

- ✔gdy osoba, której dane dotyczą, wyrazi na to **zgodę na piśmie**,
- ✔gdy **przepis szczególny innej ustawy zezwala** na przetwarzanie takich danych bez zgody osoby, której dane dotyczą i stwarza pełne gwarancje ich ochrony,
- ✔gdy przetwarzanie dotyczy danych, które są **niezbędne do dochodzenia praw przed sądem**,
- ✔gdy przetwarzanie danych jest niezbędne do wykonania zadań administratora danych odnoszących się **do zatrudnienia pracowników** i innych osób, a **zakres przetwarzanych danych jest określony w ustawie**,
- ✔gdy przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

Zasady przetwarzania danych osobowych (3)

Obowiązek dołożenia szczególnej staranności w celu ochrony osób, których dane dotyczą, tj. zachowania zasad:

✔**legalności** (przetwarzania danych zgodnie z prawem),

✔**celowości** (dane mogą być zbierane dla oznaczonych, zgodnych z prawem celów i zasadniczo niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami),

✔**merytorycznej poprawności i adekwatności** (dane powinny być poprawne, nie powinny wykraczać poza potrzeby wynikające z celu ich przetwarzania. Zakres przetwarzanych danych może wynikać np. z przepisu szczególnego, który wskazuje katalog informacji, które mogą być przetwarzane w określonym celu),

✔**czasowości** (przechowywanie danych w postaci umożliwiającej identyfikację osób, których dotyczą nie może trwać dłużej, niż jest to niezbędne do osiągnięcia celu przetwarzania).

Pamiętaj, że zakres i czas przetwarzania danych winien wynikać z celu ich przetwarzania. Masz wątpliwości? Sprawdź podstawę prawną przetwarzania danych!

Realizacja obowiązku informacyjnego, tj. obowiązek poinformowania o nazwie i adresie administratora danych, celu zbierania danych (w tym odbiorcach/kategoriach odbiorców danych), prawie dostępu do treści swoich danych oraz ich poprawiania, dobrowolności lub obowiązku podania danych (ze wskazaniem podstawy prawnej) oraz źródle danych i uprawnieniach wynikających z art. 32 ust. 1 pkt 7 i 8 ustawy o ochronie danych osobowych w przypadku zbierania danych osobowych od osoby, nie od osoby, której dane dotyczą.

Co należy wiedzieć o przesłankach legalności przetwarzania danych?

- Każda z przesłanek ma charakter **autonomiczny i niezależny** oraz są one równoprawne.
- **Zgoda** osoby, której dane dotyczą to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda **nie może być domniemana lub dorozumiana** z oświadczenia woli o innej treści. Z treści zgody powinno w sposób niebudzący wątpliwości wynikać, w jakim celu, w jakim zakresie i przez kogo dane osobowe mogą być przetwarzane. **Zgoda może być odwołana w każdym czasie**. Osoba, która wyraża zgodę nie może czuć się zmuszona do złożenia oświadczenia o wyrażeniu zgody – np. poprzez połączenie w treści oświadczenia kilku celów przetwarzania danych. Zgoda nie uprawnia do nadmiernego lub nieproporcjonalnego przetwarzania danych.
- Jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują **dalej idącą ochronę**, niż wynika to z ustawy o ochronie danych osobowych, stosuje się przepisy tych ustaw (np. zgodnie z art. 10 ust. 1 i 2 ustawy o świadczeniu usług drogą elektroniczną zakazane jest przesyłanie niezamówionej informacji handlowej skierowanej do oznaczonego odbiorcy będącego osobą fizyczną za pomocą poczty elektronicznej bez zgody odbiorcy).

Przed rozpoczęciem przetwarzania danych, w szczególności przed ich pozyskaniem, sprawdź, czy masz przesłankę legalności ich przetwarzania!

Zabezpieczenie danych osobowych (1)

Stosowanie środków technicznych i organizacyjnych, zapewniających ochronę przetwarzanych danych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczających dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

- **Środki ochrony fizycznej** – w szczególności: lokalizacja miejsc przetwarzania danych osobowych w pomieszczeniach o ograniczonym i kontrolowanym dostępie, ustalenie zasad pobierania kluczy do pomieszczeń i szaf, wyposażenie pomieszczeń, w których przetwarzane są dane osobowe, w solidne drzwi i okna, składowanie zbiorów danych osobowych (w tym nośników wymiennych i nośników kopii zapasowych) w odpowiednio zabezpieczonych szafach,
- **Środki ochrony osobowej** – w szczególności: dopuszczenie do przetwarzania danych osobowych wyłącznie osób posiadających odpowiednie upoważnienie, zapoznanych z przepisami o ochronie danych osobowych oraz obsługą systemu służącego do przetwarzania danych, ustalenie zasad wykonywania pracy i sprawowania nadzoru nad pracą praktykantów, stażystów, wolontariuszy, wykonawców umów, itp., oświadczenia o zobowiązaniu się do przestrzegania przepisów o ochronie danych osobowych, zachowania w tajemnicy przetwarzanych danych osobowych oraz informacji o sposobach ich zabezpieczenia.

Zmieniasz miejsce przetwarzania danych osobowych? Pamiętaj o obowiązku aktualizacji wykazu obszarów przetwarzania danych osobowych!

Zabezpieczenie danych osobowych (2)

- **Środki ochrony technicznej** – w szczególności: mechanizmy kontroli dostępu do systemów i zasobów, zastosowanie odpowiednich i regularnie aktualizowanych narzędzi ochronnych (programy antywirusowe, itp.), regularne tworzenie kopii zapasowych zbiorów danych przetwarzanych w systemach informatycznych,
- **Środki ochrony organizacyjnej** – w szczególności: opracowywanie i aktualizacja dokumentacji i procedur opisującej sposób przetwarzania danych osobowych, monitorowanie bezpieczeństwa danych osobowych oraz opracowywanie propozycji dotyczących doskonalenia systemów ochrony danych osobowych, wyznaczenie ABI i zastępców ABI przez ADO, koordynowanie realizacji zadań związanych z ochroną danych osobowych, sprawdzenia zgodności przetwarzania danych osobowych, stosowanie procedury w zakresie incydentów stanowiących naruszenie zasad ochrony danych osobowych.
- ✔ Administratorem bezpieczeństwa informacji (ABI) w Poczcie Polskiej S.A. jest Kierownik Zespołu Pełnomocnika ds. Ochrony Informacji Niejawnych (ZPOIN).

Przetwarzanie danych osobowych powinno być zgodne z wymaganiami określonymi w art. 36-39 ustawy o ochronie danych osobowych oraz w rozporządzeniu MSWiA w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych!

Zbiory danych osobowych

- Zbiór danych osobowych to każdy, posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie.
- **Prowadzenie rejestru zbiorów danych** przetwarzanych przez administratora, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1 ustawy, **należy do zadań ABI**.
- W przypadku powołania ABI obowiązkowi **zgłoszenia zbiorów danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych** podlega zbiór zawierający dane tzw. sensytywne (z wyłączeniem zbiorów danych zwolnionych z obowiązku rejestracji).

Planowane utworzenie zbioru danych osobowych, zmiany oraz zaprzestanie przetwarzania danych w zbiorze wymagają zgłoszenia do ABI!

Administrator danych może rozpocząć przetwarzanie tzw. danych sensytywnych w zbiorze danych po zarejestrowaniu zbioru, chyba, że zbiór podlega zwolnieniu z obowiązku zgłoszenia do rejestracji GIODO.

Prawa osoby, której dane dotyczą

- ❖ Prawo do kontroli przetwarzania jej danych osobowych, w tym:
- ✔ **prawo do informacji (art. 32 ust. 1 pkt 1-5 ustawy)** – nie częściej niż raz na 6 miesięcy,
- ✔ prawo do wniesienia pisemnego, umotywowanego **żądania zaprzestania przetwarzania jej danych w przypadkach wymienionych w art. 23 ust. 1 pkt 4 i 5 ustawy** ze względu na jej szczególną sytuację,
- ✔ **prawo do wniesienia sprzeciwu** wobec przetwarzania jej danych w przypadkach wymienionych w art. 23 ust. 1 pkt 4 i 5 ustawy, gdy administrator zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych innemu administratorowi.
- ❖ Obowiązek uzupełnienia i sprostowania danych – w razie wykazania przez osobę, której dane dotyczą, że jej dane są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane.

Przekaż bezzwłocznie do ABI wniosek w sprawie kontroli przetwarzania danych od osoby, której dane dotyczą!

Jak ograniczyć ryzyko zainfekowania złośliwym oprogramowaniem?

- Nie otwieraj automatycznie wiadomości e-mail, zawierającej nieznany odsyłacz, załącznik lub prośbę podania danych prywatnych lub służbowych - nawet jeśli został wysłany z adresu, który znasz. Pamiętaj, że cyberprzestępcy wykorzystują domeny o brzmieniu podobnym do oryginalnego (np. ipko.pl - ikpo.pl, zamiast litery „m" – „rn", np. firma.pl- firrna.pl).
- Nie otwieraj ani nie pracuj z żadnym załącznikiem, którego nie oczekiwałeś lub przeznaczenia, którego nie jesteś pewien, unikaj klikania na linki i załączniki w wiadomościach e-mail lub komunikatorach internetowych.
- Nie wykorzystuj służbowego adresu e-mail do celów prywatnych, w tym do rejestrowania się na portalach – ograniczy to ryzyko otrzymania wiadomości phishingowej (np. fałszywe powiadomienie z banku, poczty, fałszywa faktura itp.).
- Nie korzystaj z nośników danych innych osób lub nośników znalezionych (np. na parkingu), skanuj używane nośniki pod kątem złośliwego oprogramowania, uważaj na nośniki otrzymane w prezencie.
- Nie używaj tego samego hasła do wielu urządzeń oraz kont. W przypadku złamania hasła, osoba nieuprawniona będzie miała dostęp do Twoich kont i urządzeń, a także wszystkich innych, powiązanych z e-mailem (często zmiana lub reset hasła jest możliwa z wykorzystaniem adresu e-mail, podanego przy rejestracji, dlatego ważne jest posiadanie innego hasła do poczty).

Przykłady naruszenia bezpieczeństwa informacji prawnie chronionych

- Wyrzucenie do kosza niezniszczonych dokumentów zawierających dane osobowe.
- Umożliwienie pracy na własnych aktywach informacyjnych innemu pracownikowi poprzez udostępnienie swojego loginu oraz hasła.
- Wysłanie wiadomości e-mail z niezabezpieczonym plikiem Excel z danymi osobowymi pracowników na adresy e-mailowe pracowników nieupoważnionych do zapoznania się z tymi danymi.
- Wykorzystywanie danych osobowych klientów Poczty Polskiej S.A., pozyskanych z korespondencji i awizo, do celów marketingowych produktów podmiotów trzecich (bankowych, ubezpieczeniowych).
- Wykorzystanie informacji, dotyczących konkretnego pracownika UP, będącego jednocześnie klientem Banku Pocztowego S.A., do prowadzenia rozmów służbowych, których przedmiotem jest wyjaśnianie przyczyn/okoliczności brania kredytu w placówce innej niż placówka macierzysta czy omawianie takiej sytuacji z innymi pracownikami UP.
- Publikacja w Internecie (Facebook) zdjęcia kartki pocztowej z danymi adresata oraz treścią korespondencji (zdjęcie zostało wykonane przez pracownika w trakcie czynności technologicznych).

Powyższe przykłady to prawdziwe zdarzenia, które wystąpiły w Poczcie Polskiej S.A. i wiązały się z ryzykiem odpowiedzialności porządkowej lub karnej!

Przykładowe incydenty informatyczne w Poczcie Polskiej (1)

- Na elektroniczną skrzynkę służbową kierownika komórki organizacyjnej Spółki wpłynął e-mail z załącznikiem w postaci faktury Firmy X. Na skierowane przez kierownika zapytanie do Firmy X o przedmiot faktury, nadeszła odpowiedź, iż Firma X nie jest autorem przedmiotowego maila, podejrzewa włamanie na serwer swojej poczty mailowej i wysłanie wiadomości z załącznikiem zawierającym wirusa. Firma X przestrzegała przed otwieraniem załącznika. Sprawa została zgłoszona na policję. Załącznik nie został otworzony, e-mail bezzwłocznie usunięty.

Prawidłowe zachowanie pracownika zapobiegło zainfekowaniu infrastruktury teleinformatycznej Spółki.

- Do sekretariatu jednej z jednostek organizacyjnych Spółki zgłosił się znalazca pendrive, zawierającego m.in. dokumenty stanowiące tajemnicę przedsiębiorstwa, zawierające dane kontrahentów Spółki oraz prywatne materiały pracownika. Pendrive został znaleziony przez osobę postronną na dworcu. Dane służbowe zawarte na pendrive nie były zabezpieczone i umożliwiły łatwą identyfikację Poczty Polskiej S.A. jako właściciela dokumentów oraz pracownika, który zgubił pendrive. Zgodnie z wyjaśnieniami pracownika materiały służbowe zostały zgrane z laptopa na prywatny pendrive w celu skopiowania na komputer stacjonarny. Po skopiowaniu materiałów na komputer stacjonarny pracownik zapomniał o usunięciu danych.

Przetwarzanie materiałów zawierających tajemnice prawnie chronione na niezabezpieczonym prywatnym nośniku wiąże się z ryzykiem ujawnienia tych informacji oraz zainfekowania infrastruktury teleinformatycznej Spółki.

Przykładowe incydenty informatyczne w Poczcie Polskiej (2)

- Pracownik Spółki otworzył przesłaną na elektroniczną skrzynkę służbową wiadomość e-mail z załączoną fakturą, którą otworzył. W załączniku znajdowało się złośliwe oprogramowanie, które zaszyfrowało kilkadziesiąt tysięcy plików na komputerze pracownika oraz na serwerze, do którego miał dostęp. Nie udało się uzyskać dostępu do zaszyfrowanych plików.

Otworzenie otrzymanego załącznika spowodowało zainfekowanie infrastruktury teleinformatycznej Spółki oraz bezpowrotną utratę danych, w tym całej dokumentacji związanej z działalnością komórki organizacyjnej w której pracował pracownik.

- Pracownik Spółki, korzystając z Internetu w celach niezwiązanych z realizacją obowiązków służbowych (łączył się z zainfekowanymi witrynami stron muzycznych), wygenerował ruch w sieci zidentyfikowany jako połączenie z siecią botnet.

Stacja robocza pracownika mogła zostać zainfekowana złośliwym oprogramowaniem umieszczonym na zainfekowanych witrynach. Botnety mogą być wykorzystane do rozsyłania spamu, rozprzestrzeniania wirusów, atakowania komputerów i serwerów, popełniania przestępstw i oszustw.

Hasło – pierwsza linia obrony

- Pamiętaj, że trywialne hasło ułatwia atakującemu uzyskanie dostępu do informacji.
- Prawidłowe hasło powinno zawierać małe i duże litery, cyfry oraz znaki specjalne oraz składać się z minimum 8 znaków.
- Jak zbudować prawidłowe i łatwe do zapamiętania hasło? Hasło powinno różnić się od nazwy użytkownika i nie zawierać popularnych słów. Zamiast pojedynczego słowa używaj kilku słów w połączeniu z cyframi i znakami specjalnymi, stosuj zamianę znaków.
- Przykład: ułóż lub wybierz wyrażenie, które zapamiętasz, np. Iwona Bas. Wybrany zwrot możesz zapisać wspak (saB anowI).Użyj kombinacji dużych i małych liter razem ze spacją. Zamień: „a” na @, „s” na $, „i” na !, spację na %, dodatkowo literę „o” zastąp cyfrą 0, otrzymując hasło: $@B%@n0w!
- Nie wykorzystuj bezpośrednio powyższego hasła ani innych, publicznie dostępnych przykładowych haseł.
- Regularnie zmieniaj hasła i nie przechowuj ich w urządzeniach, szczególnie w formie niezaszyfrowanej.
- Nie umieszczaj hasła w łatwo dostępnym miejscu, np. przyklejone na obudowie urządzenia.

Nikomu nie udostępniaj hasła!

Podstawowe zasady bezpieczeństwa urządzeń mobilnych (1)

Pamiętaj, że samo hasło nie zapewni skutecznej ochrony Twojemu urządzeniu.

- Stosuj dodatkowe narzędzia ochrony, takie jak szyfrowanie danych.
- Zachowaj ostrożność, korzystając z urządzenia mobilnego w miejscu publicznym (osoby znajdujące się w pobliżu mogą zobaczyć wyświetlane informacje lub wpisywane hasło).
- Nie pozostawiaj urządzenia w miejscu publicznym bez nadzoru.
- Zablokuj urządzenie jeśli z niego nie korzystasz.
- Zabezpiecz swoje urządzenie, ale unikaj popularnych kodów PIN lub schematów odblokowania.
- Nigdy nie pozostawiaj niezabezpieczonego urządzenia (np. w pracy, w domu).
- Regularnie twórz kopie zapasowe wszystkich istotnych plików.
- Pamiętaj, że jailbreak (usuwanie ograniczeń) łamie podstawowy model zabezpieczeń OS i otwiera drogę dla poważnych ataków.
- Nie włączaj funkcji developerskich ani do debugowania (te funkcje dają dostęp do prywatnych danych, które w innym wypadku byłyby chronione).
- Aktualizuj oprogramowanie. Instaluj aplikacje pochodzące wyłącznie z wiarygodnych źródeł (Google Play Store, Amazon Appstore, Apple App Store, wewnętrznego korporacyjnego sklepu z aplikacjami „enterprise store”).
- Stosuj i uaktualniaj oprogramowanie antywirusowe.

Podstawowe zasady bezpieczeństwa urządzeń mobilnych (2)

- Czytaj umowy licencyjne (EULA), zanim zaakceptujesz ich warunki – unikniesz zaakceptowania warunków obniżających bezpieczeństwo.
- Staraj się nie przechowywać najważniejszych danych na mobilnych urządzeniach. Pamiętaj, że większość urządzeń mobilnych robi automatyczny backup przynajmniej części twoich danych w chmurze.
- Pamiętaj, aby przechowywane na nośniku dane były zaszyfrowane (nośniki danych łatwo zgubić lub mogą zostać ukradzione).
- Pamiętaj, żeby nie zapisywać danych na dyskach sieciowych – jak np. Google Disk.
- Nie udostępniaj nikomu służbowego urządzenia mobilnego.
- Unikaj korzystania z darmowych, niezabezpieczonych lub nieznanych sieci prywatnych WiFi (nieszyfrowana komunikacja jest łatwa do przechwycenia). Jeśli musisz użyć otwartej sieci WiFi, upewnij się, że używasz połączenia VPN, które szyfruje wszystkie przychodzące i wychodzące treści.
- Jeżeli urządzenie jest wyposażone w kamerę internetową - nie odpowiadaj na połączenia wideo od nieznajomych. Kamerę, która nie jest używana możesz zakleić.
- Uważaj - wiele programów, które wyświetlają reklamy w interfejsie użytkownika śledzi sposób reakcji użytkownika (spyware/adware).

Zapoznaj się z załączonym materiałem - BEZPIECZNE PRZETWARZANIE AKTYWÓW INFORMACYJNYCH W CHMURZE OBLICZENIOWEJ

GIODO ostrzega – aplikacje mobilne, wykorzystujące geolokalizację oraz wirtualną rzeczywistość mogą stanowić zagrożenie dla prywatności i reputacji (np. Pokemon Go, Corinth Micro Anatomy Augmented)

- Czytaj regulaminy i polityki prywatności – sprawdź, do jakich danych aplikacja będzie miała dostęp i w jakim celu. Zweryfikuj, czy Twoje dane osobowe będą przekazywane do państw trzecich.
- Czy wiesz, że aplikacja może mieć dostęp do Twoich SMS, fotografii, filmów, email, kontaktów, czatów, notatek, wpisów do kalendarza, historii przeglądanych stron, danych dotyczących karty kredytowej i płatności, biometrii (np. rozpoznanie twarzy) itp.? Pamiętaj że niektóre aplikacje mobilne, strony internetowe oraz sieci Wi-Fi mogą podczas korzystania z nich gromadzić i przesyłać informacje o lokalizacji użytkowników.
- Stosuj tryb prywatny w przeglądaniu stron w celu minimalizacji gromadzonych na urządzeniu mobilnym informacji np. o lokalizacji, o odwiedzanych stronach oraz w celu oddzielenia danych prywatnych od służbowych lub innych informacji.
- Gry i aplikacje oparte na modelu rzeczywistości wirtualnej mogą rejestrować m.in. wizerunki innych osób. Unikaj fotografowania osób trzecich w trakcie korzystania z aplikacji.
- Unikaj interaktywnych zabawek, umożliwiających inwigilację dzieci i ich otoczenia (niemiecki urząd regulacyjny informuje o przypadkach przejęcia kontroli nad zaatakowanymi urządzeniami CloudPets i użycie wbudowanych w nie kamer i mikrofonów do szpiegowania).
- Na podstawie uzyskanych w ww. sposób danych można ustalić, gdzie śpisz, pracujesz, wykryć obecność w szpitalu, miejscach o znaczeniu religijnym, obecności na demonstracjach politycznych czy w miejscach ujawniających dane dotyczące życia seksualnego (dane wrażliwe), a także tworzyć tzw. wykresy społeczne (możliwość wywnioskowania wzorców zachowania z danych dotyczących znajomych na stronach serwisów społecznościowych).

Pamiętaj!

- ✔ Nie udostępniaj informacji prawnie chronionych nieuprawnionym podmiotom!
- ✔ Nie udostępniaj informacji prawnie chronionych przez telefon, w tym danych osobowych! Podanie się przez osobę wykonującą połączenie np. za pracownika banku czy policjanta nie jest potwierdzeniem tożsamości dzwoniącego i nie zastępuje weryfikacji podstawy prawnej udostępnienia danych.
- ✔ Nie przetwarzaj danych osobowych niezgodnie z celem ich pozyskania!
- ✔ Zabezpieczaj nośniki informacji prawnie chronionych (papierowe, elektroniczne), np. w zamykanej szafce.
- ✔ Stosuj politykę czystego biurka i czystego ekranu.
- ✔ Odbieraj wydruki z drukarki niezwłocznie po wydruku.
- ✔ Skutecznie niszcz zbędne dokumenty (np. błędne wydruki), zawierające informacje prawnie chronione – nie zostawiaj ich na niszczarce.
- ✔ Chroń swoje dane do logowania.
- ✔ Hasło to pierwsza linia obrony - jest tylko Twoje. Nikomu go nie udostępniaj oraz nie przechowuj w urządzeniach, szczególnie w formie niezaszyfrowanej.
- ✔ Blokuj stację roboczą, gdy odchodzisz od stanowiska pracy.
- ✔ Przestrzegaj wymagań bezpieczeństwa informatycznego!
- ✔ Nie otwieraj żadnego załącznika, którego nie oczekiwałeś lub przeznaczenia którego nie jesteś pewien, unikaj klikania na linki i załączniki w wiadomościach e-mail.

Odpowiedzialność karna

- Nieuprawnione przetwarzanie danych osobowych zagrożone jest karą grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2 (w przypadku danych sensytywnych – do lat 3).
- Nieprawidłowe przechowywanie danych osobowych zagrożone jest karą grzywny, ograniczenia wolności albo pozbawienia wolności do roku.
- Udostępnienie danych osobom nieuprawnionym zagrożone jest karą grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2 (nieumyślnie – do roku).
- Naruszenie obowiązku zabezpieczenia danych zagrożone jest karą grzywny, ograniczenia wolności albo pozbawienia wolności do roku.
- Niezgłoszenie danych do rejestru zagrożone jest karą grzywny, ograniczenia wolności albo pozbawienia wolności do roku.
- Niedopełnienie obowiązku poinformowania zagrożone jest karą grzywny, ograniczenia wolności albo pozbawienia wolności do roku.
- Ujawnienie innej osobie lub wykorzystanie we własnej działalności gospodarczej informacji stanowiącej tajemnicę przedsiębiorstwa, jeżeli wyrządza to poważną szkodę przedsiębiorcy, zagrożone jest karą grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2.

Zmiany ram prawnych ochrony danych osobowych po 25 maja 2018 r. (1)

25 maja 2018 r. dotychczasowe krajowe regulacje prawne w zakresie ochrony danych osobowych zostaną zastąpione przez Rozporządzenie Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO).

Podstawowym celem nowych regulacji jest zapewnienie wysokiego, ujednoliconego poziomu ochrony danych w całej Unii Europejskiej, wzrost poczucia pewności prawnej w tym zakresie oraz wzmocnienie ochrony praw osób fizycznych.

Rozporządzenie przewiduje m.in. administracyjne kary pieniężne za naruszenia wskazanych w RODO przepisów w wysokości do **20 000 000 EUR** (lub do 4% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego – przy czym zastosowanie ma kwota wyższa).

W Poczcie Polskiej S.A. został powołany Zespół ds. wdrożenia przepisów RODO.

Do zadań Zespołu należy identyfikacja obszarów prac w Poczcie Polskiej S.A., wynikających z konieczności wdrożenia RODO, przygotowanie harmonogramu realizacji zadań oraz opracowanie projektów wewnętrznych aktów prawnych.

Zmiany ram prawnych ochrony danych osobowych po 25 maja 2018 r. (2)

RODO - zmodyfikowane mechanizmy ochrony danych osobowych oraz nowe rozwiązania:

- ✔Zgłaszanie naruszeń ochrony danych osobowych organowi nadzorczemu nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, chyba, że jest mało prawdopodobne, by naruszenie to skutkowało naruszeniem praw i wolności osób fizycznych, a w przypadku wysokiego ryzyka takiego naruszenia - dodatkowo obowiązek zawiadomienia osoby/osób, których naruszenie dotyczy.
- ✔Zastąpienie obowiązku notyfikacji zbiorów danych nowymi wymaganiami: obowiązkiem prowadzenia rejestru czynności przetwarzania danych osobowych i rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora.
- ✔Zmiana warunków wyrażania zgody na przetwarzanie danych osobowych: zgoda powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności, odnosić się do określonej sytuacji, być dobrowolnym, świadomym i jednoznacznym przyzwoleniem osoby, której dane dotyczą, na przetwarzanie dotyczących jej danych osobowych i która ma na przykład formę pisemnego (w tym elektronicznego) lub ustnego oświadczenia. Jeśli przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą, administrator powinien być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na operację przetwarzania. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.
- ✔Poszerzenie zakresu obowiązku informacyjnego, w szczególności o dane kontaktowe inspektora ochrony danych, informację o odbiorcach danych osobowych lub o kategoriach odbiorców - jeżeli istnieją, o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu, prawie wniesienia skargi do organu nadzorczego, informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu.

Zmiany ram prawnych ochrony danych osobowych po 25 maja 2018 r. (3)

RODO - zmodyfikowane mechanizmy ochrony danych osobowych oraz nowe rozwiązania:

- ✔Zmiana zasad powierzania przetwarzania danych osobowych: korzystanie z usług wyłącznie podmiotów zapewniających wystarczające gwarancje wdrożenia środków technicznych i organizacyjnych, na podstawie umowy, określającej przedmiot i czas trwania przetwarzania, charakter i cele przetwarzania, rodzaj danych osobowych i kategorie osób, których dane dotyczą, uwzględniającej konkretne zadania i obowiązki podmiotu przetwarzającego oraz ryzyko naruszenia praw lub wolności osoby, której dane dotyczą. Po zakończeniu przetwarzania w imieniu administratora podmiot przetwarzający powinien zwrócić lub usunąć dane osobowe, chyba że prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający, nakładają obowiązek przechowywania danych osobowych.
- ✔Obowiązek uwzględnienia ochrony danych w fazie projektowania oraz zapewnienia domyślnej ochrony danych.
- ✔Ocena skutków dla ochrony danych.
- ✔Zastąpienie ABI funkcją Inspektora Ochrony Danych.
- ✔Dodatkowe prawa osób, których dane dotyczą: prawo do „bycia zapomnianym”, prawo do ograniczenia przetwarzania danych, prawo do przenoszenia danych.
- ✔Wprowadzenie określenia: szczególne kategorie danych osobowych (dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej).

Podejmujesz działania, dotyczące danych osobowych, których skutki będą trwały po 25 maja 2018 r.? Uwzględnij wymagania RODO!

Odpowiedzi na najczęściej zadawane pytania (1)

- Czy jestem zobowiązany do zachowania tajemnicy przedsiębiorstwa także po ustaniu stosunku pracy - a jeżeli tak, to jak długo?

Zgodnie z art. 11 ust. 2 obowiązek zachowania tajemnicy przedsiębiorstwa przez pracownika trwa przez okres trzech lat od ustania zatrudnienia, chyba że umowa stanowi inaczej albo ustał stan tajemnicy. Zasadę tę stosuje się również do osób, które świadczyły pracę na podstawie innego stosunku prawnego (umowa zlecenia, umowa o dzieło, umowa agencyjna, kontrakt menedżerski, itp.). W umowie z pracownikiem lub osobą, która świadczy pracę na innej podstawie prawnej można zarówno skrócić, jak i wydłużyć omawiany okres (zachowanie tajemnicy przedsiębiorstwa może obejmować nawet czas nieograniczony, jeżeli jest to uzasadnione ochroną interesów przedsiębiorcy i nie rozciąga się na okres po ujawnieniu tajemnicy przedsiębiorstwa).

- Czy jednocześnie mogę być zatrudniona w firmie konkurencyjnej (np. na umowę zlecenie lub część etatu w InPost)?

Zakaz prowadzenia przez pracowników działalności konkurencyjnej wobec wynika wprost z kodeksu pracy (art. 100 § 2 pkt 4). Niezależnie od formy prowadzenia działalności konkurencyjnej (np. wykonywanie pracy na podstawie stosunku pracy lub umowy cywilnoprawnej na rzecz innego podmiotu; prowadzenie własnej jednoosobowej działalności gospodarczej, posiadanie udziałów lub akcji w spółkach; pełnienie funkcji członków organów osób prawnych, ich likwidatorów, syndyków, kuratorów), będzie ona miała charakter konkurencyjny, jeżeli spełnia łącznie dwa warunki: pokrywa się choćby w części z zakresem podstawowej lub ubocznej działalności pracodawcy i narusza interes pracodawcy lub mu zagraża, przy czym naruszenie lub zagrożenie musi być rzeczywiste (wyrok SA w Gdańsku z 4 lipca 2013 r.). Działalność konkurencyjna pracownika może uzasadniać rozwiązanie z nim umowy o pracę bez wypowiedzenia nawet wtedy, gdy pracodawca nie zawarł z nim umowy o zakazie konkurencji.

- Czy składając zeznania na policji, w prokuraturze lub w sądzie mogę udzielić informacji z zakresu danych osobowych i nie będę miał z tego powodu kłopotów?

Osoby zobowiązane do zachowania tajemnicy (np. pocztowej w zakresie danych podmiotów korzystających z usług pocztowych), składające zeznania/przesłuchiwane w charakterze świadka przez organy ścigania, winny zostać zwolnione z obowiązku jej zachowania (np. postanowienie prokuratora o zwolnieniu z obowiązku zachowania tajemnicy). Osoba ujawniająca tajemnicę po uprzednim zwolnieniu z obowiązku jej zachowania nie będzie ponosiła odpowiedzialności za jej naruszenie.

Odpowiedzi na najczęściej zadawane pytania (2)

- Jakich informacji może udzielić pracownik placówki pocztowej policjantowi na jego ustne żądanie?

Zgodnie z § 20 Rozporządzenia Rady Ministrów z dnia 29 września 2015 r. w sprawie sposobu postępowania przy wykonywaniu niektórych uprawnień policjantów, żądanie udzielenia niezbędnej pomocy może być zgłoszone ustnie przez każdego policjanta, który potrzebuje niezbędnej pomocy.

Policjant, zgłaszając ustnie żądanie udzielenia niezbędnej pomocy, informuje osobę, do której zgłasza żądanie w szczególności o działaniu w sytuacji niecierpiącej zwłoki albo na polecenie sądu, prokuratora lub organu administracji publicznej oraz przekazuje tej osobie podstawę prawną żądania, określenie rodzaju i zakresu niezbędnej pomocy.

Żądanie udzielenia niezbędnej pomocy zgłoszone ustnie potwierdza się niezwłocznie w sposób określony w § 19 ww. Rozporządzenia (właściwy organ Policji lub policjant działający z upoważnienia tego organu doręcza lub przekazuje żądanie drogą elektroniczną).

Ponadto, zgodnie z art. 20d ustawy z dnia 6 kwietnia 1990 r. o Policji dane dotyczące osób korzystających z usług pocztowych oraz dane dotyczące faktu i okoliczności świadczenia lub korzystania z tych usług mogą być ujawnione Policji m.in. na żądanie policjanta posiadającego pisemne upoważnienie Komendanta Głównego Policji, Komendanta CBŚP albo komendanta wojewódzkiego Policji.

Policjantowi, zgłaszającemu ustne żądanie udzielenia pomocy w ww. trybie należy udostępnić informacje zgodne z zakresem żądania.

Jeżeli policjant nie dysponuje żadną z ww. podstaw prawnych i powołuje się na np. na ogólne „potwierdzenia przypuszczenia", wówczas nie należy policjantowi udostępniać danych dotyczących osób korzystających z usług pocztowych oraz danych dotyczących faktu i okoliczności świadczenia lub korzystania z tych usług, natomiast należy poinformować, że ww. dane stanowią tajemnicę pocztową.

Poinformuj przełożonego o ustnym żądaniu udzielenia niezbędnej pomocy, zgłoszonym przez policjanta