BEZPIECZEŃSTWO DANYCH OSOBOWYCH W REALIZACJI ZLECEŃ PRZEZ BIEGŁYCH SĄDOWYCH

Szkolenie biegłych sądowych ustanowionych przy Sądzie Okręgowym w Radomiu

27 października 2021 r.

Prowadzi: Joanna Gwiazda – Inspektor Ochrony Danych Sądu Okręgowego w Radomiu

Cel szkolenia

- Zapoznanie biegłych sądowych z podstawowymi pojęciami systemu ochrony danych i najważniejszymi aktami prawnymi regulującymi ten obszar w zakresie działalności sądu polegającej na sprawowaniu wymiaru sprawiedliwości,
- Wyjaśnienie specyfiki systemu zarządzania bezpieczeństwem informacji i i ochroną danych osobowych w sądach powszechnych,
- Wyjaśnienie w jakiej roli zdefiniowanej w RODO występuje biegły sądowy przetwarzający dane osobowe w związku ze zleceniem opinii przez Sąd
- Zdefiniowanie najczęstszych zagrożeń i podatności na które narażone są dane osobowe jako aktywo niematerialne sądu powierzane biegłemu sądowemu na czas sporządzania opinii
- Rodzaje naruszeń ochrony danych i ich wpływ na prawa i wolności osób fizycznych
- Wyjaśnienie pojęcia bezpieczeństwa danych osobowych
- Omówienie dobrych praktyk, czyli próba znalezienia odpowiedzi na pytanie, jak uniknąć odpowiedzialności za naruszenie RODO

Podstawowe pojęcia systemu ochrony danych osobowych

- Dane osobowe
- Zbiór danych
- Przetwarzanie danych
- Zasady przetwarzania danych osobowych
- Dane szczególnych kategorii (wrażliwe, sensytywne)
- Ryzyko przetwarzania i analiza ryzyka
- Audyt zgodności z RODO
- Rozliczalność ze stosowania RODO
- Środki techniczne i organizacyjne
- Pseudonimizacja danych
- Szyfrowanie danych
- Ciągłość działania
- Upoważnienie do przetwarzania danych
- Uprawnienia w systemie informatycznym
- Prezes Urzędu Ochrony Danych Osobowych
- Administrator
- Podmiot przetwarzający
- Osoba upoważniona do przetwarzania danych
- Inspektor ochrony danych
- Domyślna ochrona danych
- Ochrona danych osobowych na etapie projektowania
- Prawa i wolności osób fizycznych
- Bezpieczeństwo danych osobowych
- Poufność danych
- Integralność danych
- Dostępność danych
- Incydent
- Naruszenie ochrony danych

Legalność

Zdefiniowane podstawy prawne legalizujące przetwarzanie danych osobowych,

Przestrzeganie zasad przetwarzania danych – legalności, rzetelności, przejrzystości, jawności, ograniczenia celu, ograniczenia czasu, minimalizacji przetwarzania, adekwatności danych, prawidłowości danych, poufności integralności i dostępności,

Dbałość o przekazywanie danych osobowych innym podmiotom poprzez powierzenie lub udostępnienie,

Świadomość

Budowanie świadomości zagrożeń i odpowiedzialności w organizacji

Szkolenia personelu podnoszące świadomość

Projektowanie ochrony danych na etapie projektowania danego procesu w organizacji

Włączanie Inspektora ochrony danych we wszystkie sprawy i procesy w których dochodzi do przetwarzania danych osobowych

Zabezpieczenia

Inwentaryzacja

procesów przetwarzania danych i prowadzenie aktualnego Rejestru czynności przetwarzania danych,

Zabezpieczenia IT na poziomie sprzętu i oprogramowania zgodne z charakterem przetwarzania, ryzykiem, możliwościami technicznymi i finansowymi

Rozwiązania organizacyjne w postaci wszelkich spisanych procedur, polityk bezpieczeństwa, regulaminów użytkowników systemów, polityk ochrony danych

Imienne upoważnienia do przetwarzania danych

Dokumentacja oceny skutków dla przetwarzania danych

Obowiązki wobec Urzędu Ochrony Danych Osobowych

Sformalizowane zgłaszanie wyznaczenia Inspektora ochrony danych,

Obowiązek zgłaszania naruszeń ochrony danych w organizacji w terminie 72 godzin od stwierdzenia naruszenia

Uprzednie konsultacje,

Śledzenie bieżących wytycznych i zaleceń UODO

Umożliwianie kontroli UODO w naszej organizacji

Prawa osób, których dane są przetwarzane

Obowiązki informacyjne, czyli informowanie osób których dane przetwarzamy o celu, podstawie prawnej przetwarzania ich danych, terminach usunięcia danych, ich prawach wynikających z RODO,

Prawo do wycofania zgody, przenoszenia danych, uzyskania dostępu do danych, kopii danych, prawo do usunięcia danych (tzw. prawo do bycia zapomnianym), prawo do sprzeciwu, prawo sprostowania danych i ograniczenia przetwarzania

Prawo do bycia poinformowanym o naruszeniu ochrony danych osobowych i sposobach zaradzenia konsekwencjom tego naruszenia

FILARY SYSTEMU OCHRONY DANYCH OSOBOWYCH

Najważniejsze przepisy prawa regulujące obszar ochrony danych osobowych w sądach powszechnych

Konstytucja Rzeczypospolitej Polskiej

RODO, czyli Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych

Ustawa z dnia 27 lipca 2001 r. Prawo o ustroju sądów powszechnych

Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

Inne akty prawa krajowego regulujące prawa i obowiązki podmiotów w zakresie ochrony danych osobowych, w tym Kodeks pracy, a w sektorze wymiaru sprawiedliwości Kodeks postepowania cywilnego, Kodeks Postępowania karnego, Kodeks karny wykonawczy, Regulamin urzędowania sądów powszechnych, ustawy o biegłych sądowych, mediatorach, ustawa o dostępie do informacji publicznej,

Specyfika systemu ochrony danych osobowych w sądzie powszechnym

Mnogość administratorów

- Prezes Sądu
- Dyrektor Sądu
- Sąd
- Prezes Sądu wyższej instancji
- Minister Sprawiedliwości
- Prezes Sądu Apelacyjnego realizujący zadania wynikające z zarządzenia MS

Specyfika systemu ochrony danych osobowych w sądzie powszechnym

Mnogość organów nadzorczych

Prezes Sądu wyższej instancji

Dla operacji przetwarzania danych w ramach sprawowania wymiaru sprawiedliwości zadań z zakresu ochrony prawnej w sądzie rejonowym i sądzie okręgowym

Prezes Urzędu Ochrony Danych Osobowych

W ramach operacji przetwarzania w związku z realizacją zadań przez Prezesa Sądu i Dyrektora Sądu

Krajowa Rada Sądownictwa

Dla operacji przetwarzania danych w ramach sprawowania wymiaru sprawiedliwości zadań z zakresu ochrony prawnej w sądzie apelacyjnym

Specyfika systemu ochrony danych osobowych w sądzie powszechnym

Ustawa z dnia 27 lipca 2001 r. Prawo o ustroju sądów powszechnych

Art. 175a. [Administratorzy danych osobowych]

§ 1. Administratorami danych osobowych:

1) sędziów i sędziów w stanie spoczynku oraz asesorów sądowych,

2) referendarzy sądowych, asystentów sędziów, dyrektorów sądów oraz ich zastępców, kuratorów sądowych, aplikantów aplikacji sądowej, aplikantów kuratorskich, urzędników oraz innych pracowników sądów,

3) biegłych sądowych, lekarzy sądowych, mediatorów oraz ławników,

4) kandydatów na stanowiska wymienione w pkt 1 i 2

- są prezesi i dyrektorzy właściwych sądów oraz Minister Sprawiedliwości, w zakresie realizowanych zadań.

Art. 175da. [Administratorzy danych osobowych przetwarzanych w systemach teleinformatycznych] Administratorami danych osobowych przetwarzanych w systemach teleinformatycznych obsługujących postępowania sądowe, w systemach teleinformatycznych, w których są prowadzone rejestry sądowe, oraz w systemach teleinformatycznych, w których są prowadzone urządzenia ewidencyjne (sądowe systemy teleinformatyczne), są sądy w ramach sprawowania wymiaru sprawiedliwości albo realizacji zadań z zakresu ochrony prawnej, prezesi właściwych sądów oraz Minister Sprawiedliwości w ramach realizowanych zadań.

Art. 175db. [Administratorzy danych osobowych w ramach sprawowania wymiaru sprawiedliwości albo realizacji zadań z zakresu ochrony prawnej] Administratorami danych osobowych przetwarzanych w postępowaniach sądowych w ramach sprawowania wymiaru sprawiedliwości albo realizacji zadań z zakresu ochrony prawnej są sądy.

Role w systemie – czyli kto odpowiada za RODO w zakresie operacji przetwarzania związanych ze zleceniem opinii biegłemu sądowemu

W jakiej roli zdefiniowanej w RODO występuje biegły sądowy przetwarzający dane osobowe w związku ze zleceniem opinii przez Sąd - stanowisko Urzędu Ochrony Danych Osobowych

Zgodnie ze stanowiskiem Prezesa Urzędu Ochrony Danych Osobowych wyrażonym w piśmie DOL.023.324.2021.MB.I/138964 z dnia 9 września 2021 r. kierowanym do Prezesa Sądu Okręgowego w Częstochowie biegłego należałoby uznać za administratora w sytuacji, gdy sąd zleca mu przygotowanie opinii w sprawie. Wówczas, mając konkretne dane opierając się na ustalonych faktach, biegły sam decyduje o tym jakie metody i sposoby są konieczne do tego aby wydać opinię w sprawie. Niemniej jednak ocena co do statusu biegłego i jego obowiązków związanych z realizacją zadań przypisanych mu ustawowo nie powinna następować z pominięciem reguł udostępniania danych z akt postępowania przez sąd jako administratora danych osobowych gromadzonych w tych aktach. Jeżeli realizacja zadania przez niezależnego biegłego w granicach przyznanych mu ustawowo uprawnień przebiegać będzie wyłącznie z wykorzystaniem środków technicznych i organizacyjnych biegłego (np. w ramach prowadzonej przez niego działalności gospodarczej), to ponosi on odpowiedzialność za zapewnienie zgodności procesu przetwarzania danych z przepisami o ochronie danych osobowych.

Najczęściej występujące zagrożenia i podatności rzutujące na bezpieczeństwo danych osobowych

W zakresie predyspozycji, świadomości i umiejętności osób dopuszczonych do przetwarzania danych osobowych

W zakresie sprzętu i oprogramowania

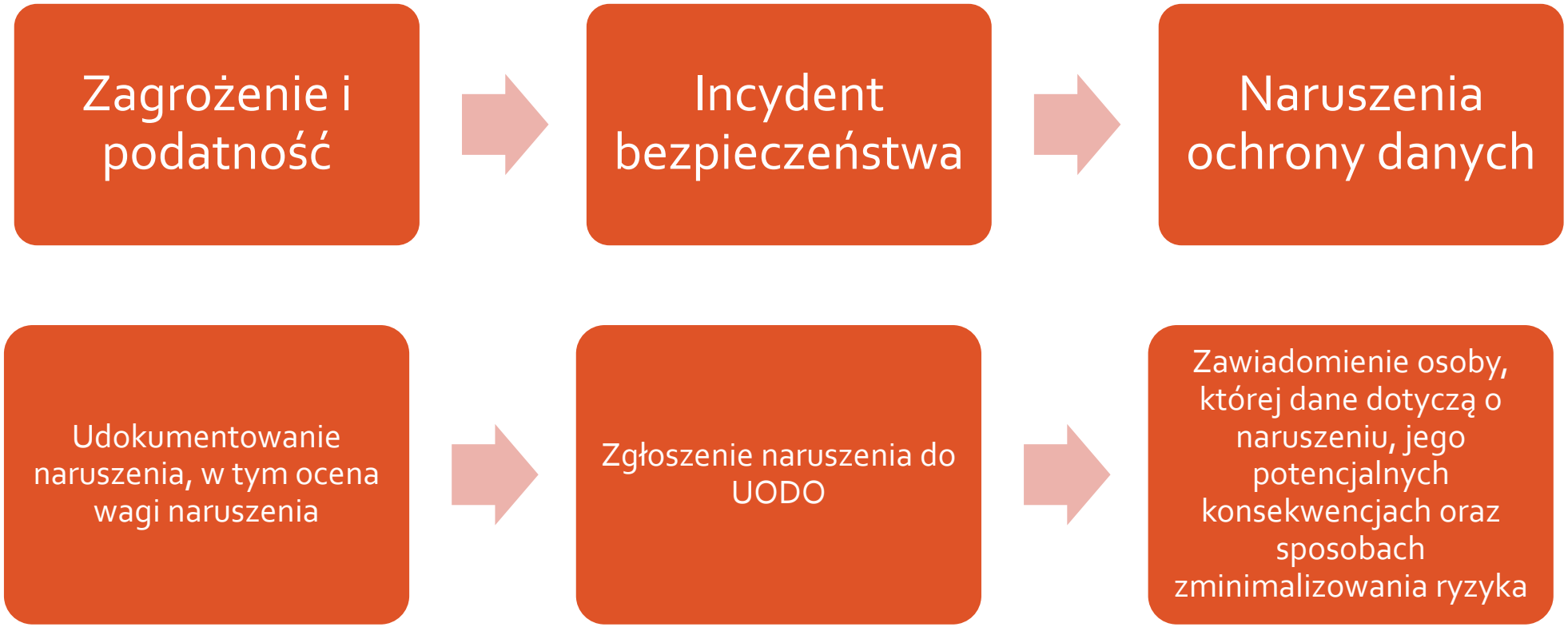
W zakresie dokumentów i obrazów zawierających dane osobowe

W zakresie pomieszczeń, w których znajdują się komputery centralne i urządzenia sieci

W zakresie pomieszczeń i infrastruktury służących do przetwarzania danych osobowych

W zakresie czynników zewnętrznych związanych z cyberbezpieczeństwem organizacji

Zagrożenia i podatności mające wpływ na bezpieczeństwo danych osobowych i obowiązki Administratora związane z ich obsługą



Rodzaje naruszeń ochrony danych i ich wpływ na prawa i wolności osób fizycznych

Administrator

przyczyna

- Brak stosowania zasad przetwarzania danych i zasad zabezpieczania danych
- Brak wiedzy o obowiązkach ochrony danych osób zaangażowanych w procesy przetwarzania danych osobowych
- Wady systemu informatycznego
- Błędy konfiguracji systemu
- Celowe działania osób zaangażowanych w procesy przetwarzania
- Klęska żywiołowa
- cyberprzestępstwo

skutek

- Przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie danych osobowych
- Nieuprawnione ujawnienie danych osobowych
- Umożliwienie nieuprawnionego dostępu do danych osobowych

Osoba fizyczna

przyczyna

- Kradzież tożsamości lub/i oszustwo z wykorzystaniem skradzionej tożsamości
- Posługiwanie się tożsamością osoby fizycznej w celu osiągnięcia korzyści majątkowej, społecznej, zawodowej, w celach powodowanych osobistymi przesłankami

skutek

- Utrata reputacji
- Dyskryminacja w środowisku społecznym, zawodowym, osobistym otoczeniu
- Stres
- Załamanie więzów rodzinnych
- Strata finansowa (zobowiązania finansowe zaciągnięte na konto osoby fizycznej, brak dostępu do konta bankowego lub utrata środków na koncie)
- Naruszenie poufności informacji chronionych tajemnicą zawodową, powodujące odpowiedzialność zawodową
- Każda inna znacząca szkoda osobista, społeczna czy gospodarcza osoby fizycznej
- Konieczność spłacania nie swoich zobowiązań do czasu wyjaśnienia sytuacji przed właściwymi organami publicznymi

Przykładowe sytuacje wykorzystania skradzionej tożsamości przedstawia film https://www.youtube.com/watch?v=ZTCBEHUuRHM

Bezpieczeństwo danych osobowych to stan, w którym administrator wykonując operacje na danych osobowych dąży do zachowania ich podstawowych atrybutów tj:

- poufności,
- integralności
- dostępności danych

Bezpieczeństwo danych osobowych na akceptowalnym poziomie można osiągnąć poprzez zapewnienie:

- analizy ryzyka i doboru adekwatnych środków organizacyjnych i technicznych w celu łatania luk systemu ochrony danych osobowych,
- ciągłości działania aktywów służących do przetwarzania danych,
- odpowiedniego poziomu świadomości osób uczestniczących w operacjach przetwarzania danych, w tym znajomości obowiązków związanych z RODO i zagrożeń powodujących naruszenia RODO
- obsługi praw podmiotów danych
- realizacji obowiązków związanych z obsługą naruszeń ochrony danych – zgłoszenie naruszenia do UODO i zawiadomienie osób, których dane dotyczą
- rozliczalności działań Administratora.

Dobre praktyki, czyli jak uniknąć naruszenia RODO podczas realizacji zleceń przez biegłego sądowego

- wiedza to bezpieczeństwo – rola świadomości i odpowiedniego poziomu wiedzy w zakresie znaczenia prawa osób fizycznych do ochrony danych osobowych i skutków braku tej świadomości,
- stosowanie w codziennej pracy zasad czystego biurka, czystego ekranu, czystego kosza (vel. zapełnionego kosza niszczarki),
- Korzystanie z usług profesjonalnych, certyfikowanych w zakresie RODO podmiotów w zakresie wspomagania pracy biegłego sądowego (drukowanie, kopiowanie, hosting poczty elektronicznej, przesyłanie pocztą lub kurierem, serwisowanie sprzętu komputerowego)
- walka z tzw. wykluczeniem cyfrowym z wyboru,
- podnoszenie kompetencji cyfrowych w związku z postępem technologicznym w każdej sferze życia (media społecznościowe, poczta elektroniczna, aplikacje mobilne, sztuczna inteligencja)
- znajomość zagrożeń związanych z funkcjonowaniem w cyberprzestrzeni i sposób na radzenia sobie z nimi,

Dobre praktyki, czyli jak uniknąć naruszenia RODO podczas realizacji zleceń przez biegłego sądowego

- Akta sądowe są kopalnią wiedzy o każdej, czasem najbardziej prywatnej sferze życia podsądnych i innych uczestników postępowania sądowego, co z punktu widzenia RODO oznacza zawsze wysokie ryzyko naruszenia praw i wolności, której dane dotyczą , a po stronie Administratora odpowiedzialność administracyjną oraz cywilną w tym zakresie,
- Traktujmy powierzone nam dane osobowe jak nasze własne,
- Unikajmy spontanicznych pośredników w trakcie przekazywania akt z opinią do sądu,
- Korzystajmy z zaufanych podmiotów świadczących usługi pocztowe i kurierskie,
- Nie zostawiajmy akt sądowych w przygodnych miejscach,
- Członek rodziny biegłego zamieszkujący w tym samym gospodarstwie domowym nie jest zgodnie z RODO osobą uprawnioną, której można ujawniać dane osobowe z akt sądowych,
- Korzystajmy z niszczarki dokumentów pozbywając się wersji roboczych czy notatek,

Dobre praktyki, czyli jak uniknąć naruszenia RODO podczas realizacji zleceń przez biegłego sądowego ciąg dalszy…

- Nie ufajmy autouzupełnianiu! Wysyłając korespondencję mailową zawsze sprawdź, czy wprowadzono adresy odpowiednich adresatów,
- Starajmy się nie wysyłać załączników zawierających dane osobowe, za każdym razem opatrzmy je hasłem, a hasła do załączników przekazujmy innym kanałem komunikacji, a nie w treści tego samego maila,
- Nie wysyłajmy zbiorczej korespondencji mailowej w taki sposób, by jej adresaci mogli wzajemnie widzieć swoje adresy mailowe. Omyłka spowoduje konieczność zgłoszenia naruszenia do UODO,
- Jeżeli można obejść się bez wysyłania danych osobowych za pośrednictwem maila, nie róbmy tego, wybierzmy bezpieczniejszą formę komunikacji,
- Zastanów się dwa razy zanim wykonasz coś metodą kopiuj – wklej; naruszając zasadę rękojmi należytego wykonywania czynności biegłego narażasz osoby fizyczne na nieuprawnione ujawnienie ich wrażliwych danych osobowych, a siebie na skreślenie z listy biegłych sądowych,
- Hasło: 1234 albo qazwsx może być za słabe, silne hasla powinny składać się z dużych i małych liter, cyfr, znaków specjalnych, zawierać minimum 8 znaków,

Dobre praktyki, czyli jak uniknąć naruszenia RODO podczas realizacji zleceń przez biegłego sądowego ciąg dalszy…

- Jeśli to możliwe korzystajmy z dwuskładnikowego uwierzytelniania w celu zabezpieczania danych osobowych,
- Panujmy nad zawartością biurka, szuflad i teczki - jeżeli nie wiesz, co się w nich znajduje to zatrzymaj się, posprzątaj i dopiero kontynuuj pracę,
- Drukujmy tylko te dokumenty, które są niezbędne do pracy,
- Jeżeli dokumenty nie są już potrzebne, usuwajmy je niezwłocznie, najlepiej wykorzystując niszczarkę, chyba że zgodnie z przepisami prawa musimy je archiwizować,
- „Nie wiem co to", „leży tu od zawsze", „w sumie to nie jest mi już potrzebne"- to podejście, które jest niedopuszczalne,
- Nie wynośmy dokumentów poza obszar bezpiecznego przetwarzania bez ich odpowiedniego zabezpieczenia,
- Zawsze bierzmy pod uwagę, że dokumenty mogą być udostępnione osobom, których dane dotyczą - nie nanosimy na nich „swobodnych" uwag i notatek

Dobre praktyki, czyli jak uniknąć naruszenia RODO podczas realizacji zleceń przez biegłego sądowego ciąg dalszy…

- Zbierajmy tylko te dane, które są niezbędne do realizacji zlecenia,
- Nie wykorzystujmy posiadanych danych osobowych w dowolnym celu - to, że już posiadamy czyjeś dane osobowe nie oznacza, że możemy z nimi zrobić wszystko, nie gromadźmy nieaktualnych danych - „przy da się" może być powodem nałożenia na Administratora na kary pieniężnej,
- Zawsze przestrzegaj ustalonych procedur i zasad ochrony danych osobowych; mogą one być uciążliwe, ale działanie na własną rękę może być droższe w skutkach niż strata 5 minut na zniszczenie stosu papierów zalegających na biurku,
- Stosujmy szyfrowanie danych podczas ich przesyłania oraz przechowywania na dysku twardym komputera czy przenośnego urządzenia pamięci masowej USB (pendrive)
- Dokumentację papierową przechowujmy w zamykanych szafach w pomieszczeniach gwarantujących dostęp jedynie osób uprawnionych i ochronę przed działaniem czynników zewnętrznych,

Dobre praktyki, czyli jak uniknąć naruszenia RODO podczas realizacji zleceń przez biegłego sądowego ciąg dalszy…

Do najpopularniejszych zagrożeń w cyberprzestrzeni należą

- 1. Użycie szkodliwego oprogramowania (wirusy, robaki, konie trojańskie, tylne wejścia, programy szpiegujące, procedury wykorzystujące znane lub ukrywane luki w programach komercyjnych).
- 2. Kradzież i wykorzystywanie cudzych danych osobowych.
- 3. Wyłudzanie, kradzież, fałszowanie lub niszczenie danych.
- 4. Blokowanie dostępu do usług (bomby pocztowe, przeciążanie aplikacji i serwisów, masowe zawłaszczanie systemów komputerowych w celu wykorzystywania ich do prowadzenia takich przeciążeń).
- 5. Przesyłanie niepotrzebnej lub niechcianej informacji.
- 6. Ataki socjotechniczne (wyłudzanie informacji poprzez podszywanie się pod instytucję lub osobę zaufaną).
- 7. Zaawansowane ataki celowane (prowadzone za pomocą wielu skoordynowanych i zindywidualizowanych metod ataki skierowane precyzyjnie przeciwko konkretnej osobie, organizacji lub firmie).

Dobre praktyki, czyli jak uniknąć naruszenia RODO podczas realizacji zleceń przez biegłego sądowego ciąg dalszy…

Jak się bronić przed zagrożeniami cyberprzestrzeni?

Należy pamiętać, że cyberprzestępcy mogą próbować oszukać swoje ofiary powołując się na autorytet instytucji publicznej, dlatego korzystając z elektronicznych usług publicznych oferowanych przez sąd oraz podczas komunikacji elektronicznej zadbaj o bezpieczeństwo swoich danych, szczególnie jeśli przetwarzasz je na urządzeniu mobilnym.

- Nigdy nie udostępniaj nikomu loginów i haseł do prywatnej lub służbowej poczty elektronicznej, portali społecznościowych, czy systemów informatycznych udostepniających usługi publiczne takich jak np. Portal Informacyjny Sądów Powszechnych, ePUAP.
- Używaj tylko silnych, indywidualnych dla każdego systemu haseł użytkownika. Korzystaj z programów antywirusowych i systematycznych aktualizacji systemów operacyjnych.
- Twoje urządzenia mobilne przechowują olbrzymią ilość wrażliwych informacji, takich jak dokumenty finansowe, zdjęcia, adresy email, dane medyczne. Korzystając z nich używaj szyfrowania i blokady ekranu, co w przypadku próby kradzieży lub zagubienia urządzenia w znacznym stopniu utrudni przestępcom dostęp do Twoich danych.

Gdzie szukać informacji z dziedziny ochrony danych osobowych i cyberbezpieczeństwa

- https://www.uodo.gov.pl
- https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo
- https://csirt.gov.pl/
- https://cyberpolicy.nask.pl/
- https://wtb.org.pl/

Ciekawe i inspirujące kanały Youtube:

https://www.youtube.com/user/ODO24pl/about
https://www.youtube.com/c/drMarlenaSakowskaBary%C5%82a/about
https://www.youtube.com/c/CzasnaRODO/about
https://www.youtube.com/c/ITwma%C5%82ejfirmie/about

Dziękuję za uwagę