Fundusze Europejskie

RODO w kontekście programu Fundusze Europejskie dla Łódzkiego 2021-2027

Robert Wakoń

rProtection
Ochrona Danych Osobowych

Fundusze Europejskie dla Łódzkiego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
ŁÓDZKIE

Agenda

Agenda

1. **Wstęp do przetwarzania – podstawy prawne ochrony danych osobowych w programie Fundusze Europejskie dla Łódzkiego 2021-2027**

- Akty prawne dotyczące przetwarzania i ochrony danych osobowych obowiązujące do dnia 25.05.2018 r. oraz ich wpływ na przetwarzanie danych osobowych w programie Fundusze Europejskie dla Łódzkiego 2021-2027
- Akty prawne dotyczące przetwarzania i ochrony danych osobowych obowiązujące od dnia 25.05.2018 r.
- Inne akty prawne

2. **Dane osobowe**

- Jakie dane należy uznać za dane osobowe
- Kategorie danych przetwarzanych w programie Fundusze Europejskie dla Łódzkiego 2021-2027

Agenda

3. **Kluczowe pojęcia dotyczące przetwarzania danych**

- Przetwarzanie danych osobowych w programie Fundusze Europejskie dla Łódzkiego 2021-2027
- Animizacja i pseudonimizacja danych
- Minimalizacja i okresy retencji danych

4. **Ogólne zasady gromadzenia i przetwarzania danych osobowych - obowiązki w zakresie ochrony danych**

- Gdzie są przetwarzane dane osobowe programie Fundusze Europejskie dla Łódzkiego 2021-2027? - Zasady specyficzne dla danych gromadzonych elektronicznie oraz papierowo lub na innych nośnikach fizycznych
- Zasady dotyczące przetwarzania danych osobowych

Agenda

5. **Poprawne wdrożenie RODO przy realizacji projektu**

- RODO w praktyce – rozliczalność i ryzyko przetwarzania danych w programie Fundusze Europejskie dla Łódzkiego 2021-2027
- Obowiązki administratora w zakresie ochrony danych w programie Fundusze Europejskie dla Łódzkiego 2021-2027
- RODO – obowiązki administratora w zakresie ochrony danych w programie Fundusze Europejskie dla Łódzkiego 2021-2027, które są możliwe do zrealizowania dzięki zaangażowaniu personelu
- Obowiązki w zakresie ochrony danych w programie Fundusze Europejskie dla Łódzkiego 2021-2027 - Rozliczalność
- Obligatoryjne środki ochrony danych - art. 32 RODO
- Omówienie technicznych oraz organizacyjnych środków ochrony oraz ich wpływ na przetwarzanie danych w projektach

Agenda

6. **Rejestr czynności/kategorii czynności przetwarzania danych osobowych**
7. **Podstawy przetwarzania danych osobowych w projektach**

- Podstawy prawne przetwarzania danych osobowych projektach - art. 6 RODO
- Podstawy prawne przetwarzania danych osobowych projektach - art. 9 RODO
- Zgoda osoby, której dane dotyczą
- Podstawy przetwarzania danych - Strona internetowa podmiotu –
- Podstawy przetwarzania danych - monitoring wizyjny –
- Dane osobowe osób małoletnich i nie tylko - podstawy przetwarzania danych w zakresie wizerunku, art. 81 ustawy o prawach autorskich –

Agenda

8. **Dobre praktyki**

- 10 Wskazówek UODO jak korzystać z praw gwarantowanych przez RODO
- 10 Wskazówek UODO, jak stosować RODO

9. **Prawa osób, których dane osobowe są przetwarzane**

- Uprawnienia osób a projekt
- Typowe ograniczenia w uprawnieniach wynikające ze specyfiki projektów

10. **Obowiązek informacyjny w programie Fundusze Europejskie dla Łódzkiego 2021-2027**
11. **Osoby i jednostki mogące uczestniczyć w przetwarzaniu danych – obowiązki i uprawnienia**

- Role „stron” przetwarzania
- Udostępnianie oraz powierzanie danych
- Umowy powierzenia danych osobowych

Agenda

12. Udostepnienie a powierzenie - różnice

- Administrator danych osobowych a procesor – kryteria rozróżnienia
- Administrator danych osobowych a procesor – najczęściej popełnianie błędy
- Administrator danych osobowych a procesor – problemy wynikające ze współpracy stron

13. Zarządzanie podmiotami przetwarzającymi (ocena wstępna, audyty)

- Wybór podmiotu przetwarzającego – komu można powierzyć dane?
- Zarządzanie podmiotami przetwarzającymi
- Warunki przetwarzania danych osobowych w projektach przez osoby upoważnione

14. Analiza przykładowej ankiety weryfikacji podmiotu przetwarzającego

Agenda

15. Inspektor Ochrony Danych

- Inspektor Ochrony Danych (IOD) i jego rola w projektach

16. Szacowanie ryzyka

- Metody przeprowadzania analizy ryzyka w ochronie danych osobowych – wytyczne normy PN-ISO/IEC 27005
- Wymagania RODO w zakresie szacowania ryzyka „hipotetycznego”
- Wykorzystywanie norm ISO w ochronie danych osobowych oraz szacowaniu ryzyka
- Proces zarządzania ryzykiem
- Szacowanie ryzyka – schemat postepowania wg normy PN-ISO/IEC 27005
- Metody określania poziomu ryzyka
- Przykłady

Agenda

- Metody określania poziomu ryzyka
- Przykłady zidentyfikowanych aktywów w procesie szacowania ryzyka
- Przykłady zidentyfikowanych zabezpieczeń w procesie szacowania ryzyka
- Przykłady występujących zagrożeń w procesie szacowania ryzyka
- Przykłady wdrożonych środków mających na celu obniżenie poziomu ryzyka w procesie szacowania ryzyka
- Działania korygujące poziom ryzyka
- Podsumowanie wraz zaleceniami dotyczącymi postępowania z ryzykiem

17. Szacowanie ryzyka rzeczywistego na przykładzie ENISY – przykład

Agenda

18. **Konsekwencje niewłaściwego stosowania przepisów RODO w programie Fundusze Europejskie dla Łódzkiego 2021-2027**

- Ogólne warunki nakładania administracyjnych kar pieniężnych i ich zależność od świadomości oraz postawy personelu
- RODO to nie fikcja – nałożone kary w Polsce
- RODO to nie fikcja – zgłoszone skargi i naruszenia
- Pamiętaj!!!

19. **Konsekwencje niewłaściwego stosowania przepisów RODO w programie Fundusze Europejskie dla Łódzkiego 2021-2027 - co robić aby ich uniknąć - RODO a Cyberbezpieczeństwo dlaczego te obszary są nierozłączne**

- Wdrożone zabezpieczenia vs świadomość w zakresie bezpieczeństwa
- Wektory wejścia
- Zagrożenia
- Podstawowe zasady bezpieczeństwa

Agenda

20. **Obsługa naruszeń przy przetwarzaniu danych**
- Naruszenie czy incydent? – art. 33
- Obowiązki w zakresie zgłaszania naruszeń

21. **Omówienie formularza zgłoszenia naruszenia do UODO**

22. **Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych – art. 34 – przykład**

23. **Dobre praktyki przy przetwarzaniu danych osobowych**

24. **Korzystanie ze służbowej poczty email**

25. **Korzystanie ze służbowego komputera**

Wstęp do przetwarzania – podstawy prawne ochrony danych osobowych w programie Fundusze Europejskie dla Łódzkiego 2021-2027

Akty prawne dotyczące przetwarzania i ochrony danych osobowych obowiązujące do dnia 25.05.2018 r. oraz ich wpływ na przetwarzanie danych osobowych w programie Fundusze Europejskie dla Łódzkiego 2021-2027:

- **Konstytucja Rzeczpospolitej Polskiej** z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 r. Nr 78, poz. 483).
- Ustawa z dnia 29 sierpnia 1997 o Ochronie Danych Osobowych(Dz.U. z 2016 r poz. 922 ze zm.).
- **Rozporządzenie Ministra Spraw Wewnętrznych i Administracji** z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 200N4 r. r 100, poz. 1024).
- **Rozporządzenie Ministra Spraw Wewnętrznych i Administracji** z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. z 2008 r. Nr 229, poz. 1536).

Akty prawne dotyczące przetwarzania i ochrony danych osobowych obowiązujące od dnia 25.05.2018 r.

- 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
- DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW
- Ustawa z dnia 10 maja 2018 r. O Ochronie Danych Osobowych
- Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania RODO

Inne akty prawne

- ustawa z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027 – ustawa wdrożeniowa
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2021/1060 z 24 czerwca 2021 r
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1057 z dnia 24 czerwca 2021 r. ustanawiające Europejski Fundusz Społeczny Plus (EFS+)
- Ustawa z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027

Fundusze Europejskie

Dane osobowe

Jakie dane należy uznać za dane osobowe

- Dane osobowe” oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
- Informacji nie uważa się za umożliwiającą określenie tożsamości, jeżeli wymagałoby to nadmiernych kosztów, czasu i działań.
- Danymi osobowymi nie są pojedyncze informacje o dużym stopniu ogólności, np. sama nazwa ulicy i numer domu.

Kategorie danych przetwarzanych w programie Fundusze Europejskie dla Łódzkiego 2021-2027

- imię
- nazwisko
- adres zamieszkania
- PESEL
- NIP
- numer i seria dowodu osobistego
- wykształcenie
- zawód
- płeć
- numer telefonu

Dane zwykłe

- pochodzenie rasowe lub etniczne
- poglądy polityczne
- przekonania religijne lub światopoglądowe
- przynależność do związków zawodowych
- informacja o stanie zdrowia
- dane biometryczne, genetyczne
- seksualność
- orientacja seksualna

Art. 10 RODO

- wyroki skazujące
- czyny zabronione

Szczególna kategoria danych

(sensytywne, szczególnie chronione)

Kluczowe pojęcia dotyczące przetwarzania danych

Przetwarzanie danych osobowych w programie Fundusze Europejskie dla Łódzkiego 2021-2027

Operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Animizacja i pseudonimizacja danych

- Skuteczna animizacja danych
  - dobre praktyki
  - najczęściej popełniane błędy
- Skuteczna pseudonimizacja danych
  - dobre praktyki
  - najczęściej popełniane błędy

Minimalizacja i okresy retencji danych

- Minimalizacja danych
  - dobre praktyki
  - najczęściej popełniane błędy
- Okres retencji danych
  - dobre praktyki
  - najczęściej popełniane błędy

Ogólne zasady gromadzenia i przetwarzania danych osobowych - obowiązki w zakresie ochrony danych

Gdzie są przetwarzane dane osobowe w programie Fundusze Europejskie dla Łódzkiego 2021-2027? - Zasady specyficzne dla danych gromadzonych elektronicznie oraz papierowo lub na innych nośnikach fizycznych

01

w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych

02

w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych

Zasady dotyczące przetwarzania danych osobowych

Dane osobowe muszą być:

- Przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą,
- Zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami,
- Adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”),
- Prawidłowe i w razie potrzeby uaktualniane,
- Przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, **przez okres nie dłuższy, niż jest to niezbędne do celów**, w których dane te są przetwarzane,
- Przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych.

Poprawne wdrożenie RODO przy realizacji projektu

RODO w praktyce – rozliczalność i ryzyko przetwarzania danych w programie Fundusze Europejskie dla Łódzkiego 2021-2027

- Rozszerzenie pojęcia danych osobowych, tak że uwzględnia ono możliwość rozwoju technologicznego, np. uwzględnienie danych biometrycznych, genetycznych.
- **Podejście oparte na ryzyku – im mniej potencjalnych zagrożeń dla danych, tym mniej obowiązków ciąży na podmiocie, który przetwarza dane.**
- Obligatoryjne w wielu przypadkach – **powołanie Inspektora Ochrony Danych (DPO).**
- Wysokie kary pieniężne (do 20 mln euro) lub do 4% obrotu przedsiębiorstwa z poprzedniego roku, nakładane przez Urząd Ochrony Danych, **w przypadku jednostek budżetowych kara ma wynosić maksymalnie 100 000 zł.**
- Nowy obowiązek informacyjny.
- Nowe pojęcia dotyczące danych i procesów przetwarzania: ograniczenie przetwarzania, profilowanie, pseudonimizacja, anonimizacja.

Obowiązki administratora w zakresie ochrony danych w programie Fundusze Europejskie dla Łódzkiego 2021-2027

- Art. 35 RODO – przeprowadzenie Oceny Skutków dla ochrony danych (Analiza Ryzyka, czyli ocena ryzyk, jakie mogą pojawić się przy przetwarzaniu danych osobowych).
- Art. 30 RODO – prowadzenie rejestru czynności przetwarzania, zawierającego informacje co, gdzie, w jakim celu, w jakim zakresie, kategorie osób i odbiorców, przekazywanie danych do państwa trzeciego, środki techniczne i organizacyjne.
- Wdrożenie polityk ochrony danych, których zadaniem jest dokonanie podsumowania zasad panujących administracji publicznej, dotyczących procesów przetwarzania.
- Stosowanie zasady, zgodnie z art. 25 ust. 1, w myśl której już na etapie projektowania systemu oraz na etapie stosowania go należy zabezpieczyć odpowiednie środki techniczne i organizacyjne (*privacy by design*).
- Stosowanie zasady *privacy by default*, (art. 25 ust. 2), w myśl której administrator zobowiązany będzie wdrożyć takie środki techniczne i organizacyjne, aby domyślnie przetwarzane były tylko te dane osobowe, które są niezbędne do osiągnięcia celu przetwarzania.

RODO – obowiązki administratora w zakresie ochrony danych w programie Fundusze Europejskie dla Łódzkiego 2021-2027, które są możliwe do zrealizowania dzięki zaangażowaniu personelu

- Notyfikacja naruszeń związanych z ochroną danych do organu w ciągu 72 h. Obowiązkiem powiadomień objęty jest również podmiot przetwarzający, który bez zbędnej zwłoki będzie musiał zawiadomić ADO o naruszeniach.
- Stosowanie nowych klauzul do dokumentacji, umów wg nowych wytycznych.
- Realizacja nowych praw osoby której dane dotyczą.
- Jeżeli przetwarzanie odbywa się na podstawie zgody to na ADO spoczywać będzie obowiązek wykazania, że osoba której dane dotyczą wyraziła zgodę na przetwarzanie.

Obowiązki w zakresie ochrony danych w programie Fundusze Europejskie dla Łódzkiego 2021-2027 - Rozliczalność

- Szacowanie ryzyka a zakres wdrożone dokumentacji oraz środków – metodyka szacowania ryzyka, typy ryzyk (hipotetyczne, rzeczywiste).
- Udokumentowanie wdrożenia adekwatnych środków technicznych i organizacyjnych.
- Dokumentowanie procesów przetwarzania – rejestry czynności oraz rejestry kategorii czynności.
- Wdrożenie odpowiednich polityk ochrony danych.
- Prowadzenie rejestrów umów powierzenia oraz udostępnień danych osobowych.
- Stworzenie odpowiednich procedur realizacji praw osób, których dane dotyczą – odpowiedzialność, zasady komunikacji z podmiotem danych, zasady realizacji praw podmiotu danych.

Obligatoryjne środki ochrony danych - art. 32 RODO

- Wdrożenie adekwatnych środków technicznych i organizacyjnych – pseudonimująca, szyfrowanie.
- Zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania.
- Zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.
- Regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych.
- Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Omówienie technicznych oraz organizacyjnych środków ochrony oraz ich wpływ na przetwarzanie danych w projektach

- Środki ochrony fizycznej danych
- Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej
- Środki ochrony w ramach narzędzi programowych i baz danych
- Środki organizacyjne

Rejestr czynności/kategorii czynności przetwarzania danych osobowych

Rejestr czynności/kategorii czynności przetwarzania

- Zakres danych zawartych w rejestrze
- Forma prowadzenia rejestrów czynności - **przykłady**
- Rejestr kategorii czynności przetwarzania

Podstawy przetwarzania danych osobowych w projektach

Podstawy prawne przetwarzania danych osobowych projektach - art. 6 RODO

- Osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów – art. 6 ust. 1 lit a.
- Przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy 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 – art. 6 ust. 1 lit b
- Przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze – art. 6 ust. 1 lit c.
- Przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej – art. 6 ust. 1 lit d.
- Przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi – art. 6 ust. 1 lit e.

Podstawy prawne przetwarzania danych osobowych projektach - art. 6 RODO

- Przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem. Akapit pierwszy lit. f) nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań. 2. – art. 6 ust. 1 lit f.

Podstawy prawne przetwarzania danych osobowych przez służby zatrudnienia - art. 9 RODO

- Osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów – art. 9 ust. 2 lit a.
- Przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze – art. 9 ust. 2 lit b.
- Przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej – art. 9 ust. 2 lit c.
- Przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych – art. 9 ust. 2 lit d.
- Przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą – art. 9 ust. 2 lit e.

Podstawy prawne przetwarzania danych osobowych przez służby zatrudnienia - art. 9 RODO

- Przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy – art. 9 ust. 2 lit f.
- Przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego – art. 9 ust. 2 lit g.
- Przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego – art. 9 ust. 2 lit h.
- Przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych – art. 9 ust. 2 lit i.

Podstawy prawne przetwarzania danych osobowych przez służby zatrudnienia - art. 9 RODO

- Przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 – art. 9 ust. 2 lit j.

Zgoda osoby, której dane dotyczą

- Zabronione jest automatyczne zaznaczanie zgody – zgoda musi być dobrowolna, konkretna oraz świadoma.
- Zakaz łączenia zgód na przetwarzanie danych (np. zgoda na przetwarzanie danych w celach marketingowych ze zgodą na przesyłanie drogą elektroniczną).
- Klauzula zgody musi być jasna i przejrzysta, zgoda musi dotyczyć konkretnego celu
- Odrębna zgoda dla każdego celu przetwarzania.
- Zgoda musi być wyrażona bez przymusu.

Zgoda osoby, której dane dotyczą

- **Zgoda osoby której dane dotyczą:**
  - okazanie woli – dane zwykłe – CV,
  - działanie dobrowolne, konkretne, świadome i jednoznaczne – dane zwykłe,
  - w formie oświadczenia, zgoda wyraźna – dane szczególnej kategorii oraz profilowanie.

- Zgoda na przetwarzanie danych musi być wyraźna. Nie spełnia tego wymagania podpisanie oświadczenia o wyrażeniu zgody na przetwarzanie danych, stanowiącego dodatkowy element innego zobowiązania niezawierającego informacji o celach i zakresie przetwarzania danych.
- Zgoda musi mieć charakter wyraźny, a jej wszystkie aspekty muszą być jasne dla podpisującego w momencie jej wyrażania. Czynności takiej nie konwaliduje późniejsze poinformowanie o treści regulaminu, ani możliwość zgłoszenia zastrzeżeń wobec pewnych form przetwarzania danych.(wyrokNSAz4.4.2003r.,IISA2135/02).

Podstawy przetwarzania danych
- Strona internetowa podmiotu -

- Pliki Cookie:
  - reklamowe,
  - klasyczne.
- Prawo Komunikacji Elektronicznej:
  - kara – postępowanie karne – 5000 zł,
  - kara – postępowanie administracyjne 3% lub 1 000 000 zastosowanie ma wyższa,
  - zgoda każdej osoby – nie może pracodawca wyrazić zgody w imieniu pracowników,
  - zgoda na marketing bezpośredni oraz niezamówione informacje handlowe.
- WCAG 2.1 - Web Content Accessibility Guidelines

Podstawy przetwarzania danych
- monitoring wizyjny -

- Zasady przetwarzania danych:
  - podstawa prawna (art. 9a Ustawą z dnia 8 marca 1990 r. o samorządzie gminnym),
  - okres retencji,
  - zmiany w nowelizacji RODO.
- Zasady udostępniania nagrań z monitoringu:
  - udostępnienie wnioskodawcy,
  - ograniczenie przetwarzania,
  - ograniczenie przetwarzania -> PUODO.

Dane osobowe osób małoletnich i nie tylko - podstawy przetwarzania danych w zakresie wizerunku, art. 81 ustawy o prawach autorskich –

- Czy wizerunek to dana osobowa?
- Podstawa prawna przetwarzania wizerunku
- Zgoda na przetwarzanie wizerunku
- Wyjątki w zakresie przetwarzania danych w zakresie wizerunku
  - pełnienie funkcji publicznych,
  - osoba jako szczegół całości.

Dobre praktyki

10 Wskazówek UODO jak korzystać z praw gwarantowanych przez RODO

- ❑ **Każdy ma prawo wiedzieć, co będzie się działo z jego danymi.**
- ❑ **Każdy ma prawo w każdej chwili wycofać zgodę.**
- ❑ **Informacja o przetwarzaniu danych powinna być przekazywana w sposób jasny i zrozumiały.**
- ❑ **Nie ze wszystkich praw osoba której dane dotyczą może skorzystać.**
- ❑ **Każda osoba której dane dotyczą ma prawo do informacji o naruszeniu jej danych.**
- ❑ **Jeżeli zostanie wniesiony sprzeciw - marketing nie może być prowadzony.**
- ❑ **Należy chronić dzieci przed nieuczciwymi praktykami.**
- ❑ **Realizacji praw osoba której dane dotyczą najpierw powinna żądać od administratora.**
- ❑ **Każda osoba której dane dotyczą może dochodzić swoich praw przed sądem.**
- ❑ **Każda osoba ma prawo złożyć skargę do UODO.**

- https://uodo.gov.pl/pl/171/579
- https://archiwum.uodo.gov.pl/pl/138/588

10 Wskazówek UODO, jak stosować RODO

- ❑ **Ustal właściwą podstawę zbierania i wykorzystywania danych osobowych.**
- ❑ **Dopełniaj obowiązku informacyjnego zgodnie z nowymi zasadami.**
- ❑ **Komunikuj się w sposób przejrzysty.**
- ❑ **W każdej sytuacji dbaj o respektowanie praw osób.**
- ❑ **Pamiętaj, że zgoda może być wycofana w każdym momencie.**
- ❑ **Naruszenia ochrony danych zgłaszaj do Prezesa UODO, a gdy trzeba informuj o nich również osoby, których dane zostały naruszone.**
- ❑ **Nie twórz niepotrzebnej dokumentacji.**
- ❑ **Masz prawo profilować, ale pamiętaj o ograniczeniach.**
- ❑ **Zainwestuj w fachowego IOD.**
- ❑ **Uważaj na oszustów.**

- https://uodo.gov.pl/pl/171/578
- https://archiwum.uodo.gov.pl/pl/383/578

Prawa osób, których dane osobowe są przetwarzane

Prawa osób a projekt

- Prawo dostępu:
  - prawo do informacji o przetwarzaniu danych,
  - prawo do kopii danych.
- Prawo do sprostowania.
- Prawo do usunięcia (prawo dobycia zapomnianym) – poinformowanie innych administratorów.
- Prawo do ograniczenie przetwarzania.
- Prawo do przenoszenia, stanowiące istotne wyzwanie organizacyjne i techniczne (art. 6 ust. 1 lit a, b; art. 9 ust. 2 lit a).
- Prawo sprzeciwu (art. 6 ust. 1 lit e, f; marketing bezpośredni).
- Prawo wniesienia skargi do Urzędu Ochrony Danych.
- Art. 82 RODO pozwala na żądanie odszkodowania od ADO za szkody majątkowe i niemajątkowe w myśl KC art. 23 i 24 dotyczącego naruszenia dóbr osobistych.

Prawa osób a projekt

- Bezpłatny dostęp do danych osobowych.
- Miesiąc na odpowiedź:
  - realizacja żądania,
  - odmowa realizacji żądania,
  - informacja o przedłużeniu realizacji żądania,
  - powtarzające się żądania.
- Przejrzystość – Art. 12 Administrator podejmuje **odpowiednie środki**, aby w **zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem** – w szczególności gdy informacje są kierowane do dziecka – udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14, oraz prowadzić z nią wszelką komunikację na mocy art. 15–22 i 34 w sprawie przetwarzania. Informacji udziela się **na piśmie lub w inny sposób**, w tym w stosownych przypadkach – elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji **można udzielić ustnie**, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.

Typowe ograniczenia w uprawnieniach wynikające ze specyfiki projektów

- Zależności pomiędzy prawami osób których dane dotyczą a podstawami przetwarzania danych osobowych:
  - przetwarzanie na podstawie zgody, a prawa osób,
  - przetwarzanie na podstawie umowy, a prawa osób,
  - przetwarzanie na podstawie obowiązku prawnego, a prawa osób,
  - przetwarzanie na podstawie interesu publicznego, a prawa osób
  - przetwarzanie na podstawie uzasadnionego interesu a prawa osób,
  - test równowagi.

Obowiązek informacyjny w programie Fundusze Europejskie dla Łódzkiego 2021-2027

RODO – Obowiązek informacyjny

- Dane uczestników projektu a dane osób zatrudnionych na projekcie
- Dane zbierane bezpośrednio od osób, których dane dotyczą
- Dane zbierane nie od osób, których dane dotyczą
- Dane zbierane od wykonawców lub kontrahentów – kontakty robocze

RODO – Obowiązek informacyjny

- Zbieranie danych od osoby, której dane dotyczą – art. 13 RODO.
- Zbieranie danych z innych źródeł – art. 14.
- **Warstwowe spełnianie obowiązku informacyjnego -** pierwsza warstwa powinna zawierać (EROD):
  - nazwę i dane kontaktowe administratora,
  - cel i podstawy przetwarzania,
  - prawa osób których dane dotyczą,
  - odesłanie do pełnego obowiązku, np. na stronie www.
- **Ograniczenia obowiązku z art. 13**
  - jedynie gdy i w zakresie, w jakim zakresie osoba, której dane dotyczą, dysponuje już tymi informacjami

RODO – Obowiązek informacyjny

- **Ograniczenia obowiązku z art. 14:**
  - osoba, której dane dotyczą, dysponuje już tymi informacjami,
  - udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku,
  - pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą,
  - dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.

RODO – Obowiązek informacyjny

Art. 24 UODO	Art. 13 RODO
✓Adres siedziby i pełna nazwa ✓Cel zbierania danych ✓Odbiorcy lub kategorie odbiorców ✓Prawo dostępu do treści swoich danych oraz ich poprawiania ✓Informacja o dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej	✓Tożsamość administratora i dane kontaktowe ✓Dane kontaktowe IOD ✓Cel przetwarzania i **podstawa prawna** ✓**Prawnie uzasadniony interes** ✓Odbiorcy danych lub kategorie odbiorców ✓**Przekazanie danych do państwa trzeciego** ✓**Okres przechowywania** ✓Prawa osób ✓Odwołanie zgody ✓**Prawo do złożenia skargi** ✓Informacja o obowiązku lub dobrowolności podania danych i konsekwencjach niepodania danych ✓**Zautomatyzowane podejmowanie decyzji**

RODO – Obowiązek informacyjny

Art. 25 UODO	Art. 14 RODO
✓Adres siedziby i pełna nazwa ✓Cel zbierania danych ✓Zakres danych ✓Odbiorcy lub kategorie odbiorców ✓Źródło danych ✓Prawo dostępu do treści swoich danych oraz ich poprawiania ✓Prawo sprzeciwu	✓Tożsamość administratora i dane kontaktowe ✓Dane kontaktowe IOD ✓Cel przetwarzania i **podstawa prawna** ✓**Prawnie uzasadniony interes** ✓Odbiorcy danych lub kategorie odbiorców ✓Kategorie danych ✓**Przekazanie danych do państwa trzeciego** ✓**Okres przechowywania** ✓Źródło danych ✓Prawa osób ✓**Odwołanie zgody** ✓**Prawo do złożenia skargi** ✓**Zautomatyzowane podejmowanie decyzji**

RODO – Obowiązek informacyjny

Przy czynności doprecyzowania celów przetwarzania danych osobowych należy mieć na uwadze to, że późniejsza zmiana lub rozszerzenie wskazanego w danej klauzuli celu przetwarzania danych osobowych spowoduje konieczność ponownego wykonania obowiązku informacyjnego.

Dopuszczalne formy spełnienia obowiązku informacyjnego:

- pisemna,
- elektroniczna,
- ustna, na życzenie osoby,
- warstwowa.

RODO – Obowiązek informacyjny

Najczęściej popełniane błędy:

- nieprawidłowo wskazany administrator danych,
- nieprawidłowy katalog aktów prawnych, wskazywanych przy przesłance legalności przetwarzania z art. 6 ust. 1 lit. c) RODO,
- umieszczanie w katalogu aktów prawnych, odnoszących się do przesłanki z art. 6 ust. 1 lit. c) RODO, dokumentów niebędących aktami prawnymi,
- wskazywanie zgody osoby, której dane dotyczą [art. 6 ust. 1 lit. a) RODO, jako przesłanki legalności przetwarzania danych w przypadku kiedy podstawą przetwarzania nie jest zgoda,
- niedopasowanie katalogu praw przysługujących podmiotowi danych do przesłanek legalności przetwarzania danych.

Osoby i jednostki mogące uczestniczyć w przetwarzaniu danych – obowiązki i uprawnienia

Role „stron” przetwarzania

- **Administrator** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.
- **Podmiot przetwarzający** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.
- **Odbiorca** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe.
- **Współadministrator** - jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami.

Udostępnianie oraz powierzanie danych

- Kiedy powinna być zawarta umowa powierzenia danych – art. 28?
- Po czyjej stronie leży obowiązek podpisania umowy powierzenia?
- Kiedy powinna być zawarta umowa udostępnienia danych?
- **Udostepnienie na wniosek - zasady**
- Przetwarzanie na podstawie upoważnienia oraz oświadczenia o zachowaniu w poufności.
- Upoważnienie do przetwarzania danych przed i po nowelizacji RODO.
  - upoważnienia do przetwarzania danych a obowiązki służbowe – kiedy dodatkowe upoważnienia?

Umowy powierzenia danych osobowych

- Rodzaje umów

  - standardowa klauzula dot. powierzenia danych – przykład

  - umowa „własna”

- **Przykładowa umowa powierzenia danych**

Udostepnienie a powierzenie - różnice

Udostepnienie a powierzenie - różnice

	Powierzenie przetwarzania	Udostępnienie
Odbiorca danych osobowych	**Procesor/Podmiot przetwarzający** - przetwarza dane osobowe **w imieniu administratora danych** i w ramach zlecenia administratora powierzającego przetwarzanie	**Inny administrator danych** - przetwarza dane **w imieniu własnym**, decyduje o celach i sposobach przetwarzania
Podstawa prawna przetwarzania po stronie odbiorcy	**Umowa** powierzenia przetwarzania danych osobowych	Jedna z przesłanek przetwarzania określona w **przepisie art. 6 ust. 1 RODO**: zgoda/wykonanie umowy/obowiązek prawny/ochrona żywotnych interesów/zadanie realizowane w interesie publicznym/prawnie uzasadniony interes
Obowiązek informacyjny po stronie odbiorcy	**Brak** – procesor nie ma obowiązku informacyjnego wobec osoby, której dane dotyczą	**Takie jak administratora** – określone w art. 13 i 14 RODO
Retencja danych osobowych po stronie odbiorcy	Co do zasady, **do czasu obowiązywania umowy** z administratorem	Do czasu **osiągnięcia celów przetwarzania**

Administrator danych osobowych a procesor – kryteria rozróżnienia

- Stopień samodzielności w podejmowaniu decyzji o celach i środkach przetwarzania danych osobowych.
- Występowanie wobec osób trzecich jako strona umowy.
- Inne okoliczności (kto jest właścicielem bazy danych itp.).

Administrator danych osobowych a procesor – najczęściej popełnianie błędy

- Powierzenie danych w sytuacji kiedy do powierzenia nie dochodzi.
- Stosowanie się do zasad obowiązujących w 2018 – ze wszystkimi podpisuje się umowy powierzenia danych.
- Brak weryfikacji zapisów w zawartych umowach powierzenia danych.
- Akceptacja niekompletnych umów, które nie zwierają wszystkich obligatoryjnych zapisów.

Administrator danych osobowych a procesor – problemy wynikające ze współpracy stron

- Brak reakcji ze strony administratora pomimo chęci podpisania umowy powierzenia przez procesora.
- Niewłaściwe zapisy w umowie powierzenia danych narzucane przez procesora.
- Brak włączania Inspektora Ochrony Danych przed podpisaniem umowy.

Zarządzanie podmiotami przetwarzającymi (ocena wstępna, audyty)

Wybór podmiotu przetwarzającego – komu można powierzyć dane?

- Art. 28 ust 1 RODO - Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą.

Zarządzanie podmiotami przetwarzającymi (ocena wstępna, audyty)

- Czy oświadczenie podmiotu przetwarzającego w zakresie wdrożenia adekwatnych środków technicznych i organizacyjnych jest wystarczające?
- Czy zapisy ograniczające prawo kontroli przez Administratora są dopuszczalne.
- Kto decyduje o sposobie weryfikacji podmiotu przetwarzającego?

Analiza przykładowej ankiety weryfikacji podmiotu przetwarzającego

Warunki przetwarzania danych osobowych w projektach przez osoby upoważnione

Osoba upoważniona może przetwarzać dane, tylko i wyłącznie w sytuacji, gdy:

- Zapoznała się z przepisami dotyczącymi ochrony danych osobowych, w tym z procedurami instrukcjami wprowadzonymi do stosowania przez Zarządzenie Zarządu
  - regulamin służbowej poczty email,
  - regulamin użytkowania komputera służbowego,
  - politykami ochrony danych osobowych.
- Posiada pisemne **upoważnienie** do przetwarzania danych osobowych.
  - upoważnienie do przetwarzania danych - przykład
- Jest umieszczona **w Ewidencji Osób Upoważnionych** do przetwarzania danych:
  - **z określeniem celu i zakresu** wskazanym w upoważnieniu,
  - przez **okres** na jaki upoważnienie zostało udzielone.

Osoba upoważniona może przetwarzać dane, tylko i wyłącznie w sytuacji, gdy:

- **Uwaga!** Osoby upoważnione do przetwarzania danych osobowych są zobowiązane do ochrony danych zarówno w trakcie trwania zatrudnienia, jak i po jego ustaniu.
- Zachowanie w tajemnicy, o której mowa w art. 28 ust. 3 lit. b) RODO danych osobowych, zarówno w trakcie trwania stosunku prawnego łączącego osobę zpodmiotem przetwarzającym, jak i po jego ustaniu.
  - oświadczenie o zachowaniu w poufności – przykład.
- Zabezpieczenia dokumentów przed dostępem osób nieupoważnionych do przetwarzania danych osobowych, przetwarzaniem z naruszeniem ustawy, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem, a także przenoszeniem dokumentów poza miejsce ich przetwarzania.

Inspektor Ochrony Danych

Inspektor Ochrony Danych (IOD) i jego rola w projektach

Obowiązek powołania

- Przetwarzania dokonują organ lub podmiot publiczny (zgodnie z Kodeksem Postępowania Administracyjnego), z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości.
- Główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę (główna działalność zgodnie z motywem 97 RODO – przetwarzanie jest główną działalnością administratora, jeżeli oznacza jego zasadnicze, a nie poboczne czynności).
- Główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10.

RODO – Inspektor Ochrony danych IOD

- Z obsługi jednego IOD może korzystać wielu ADO (nie mogą korzystać duże podmioty znacznie oddalone od siebie).
- Wyznaczając jednego IOD dla kilku podmiotów należy uwzględnić, że musi być on dla nich łatwo dostępny.
- Art. 37 ust. 6 RODO - Inspektor ochrony danych może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług.
- Art. 37 ust 5 RODO - Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej.
- Administrator lub podmiot przetwarzający publikują dane kontaktowe inspektora ochrony danych i zawiadamiają o nich organ nadzorczy.
- ADO i podmiot przetwarzający zostali zobowiązani do zapewnienia Inspektorowi zasobów niezbędnych do utrzymania jego wiedzy fachowej.

RODO – Inspektor Ochrony danych IOD

- IOD musi podlegać bezpośrednio najwyższemu kierownictwu spółki – gwarancja niezależności i unikanie konfliktu interesów.
- IOD musi być włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
- IOD powinien być w stanie wykonywać swoje obowiązki w sposób niezależny (motyw 97 RODO) (zakaz wydawania instrukcji w zakresie realizacji zadań, brak możliwości ukarania odwołania i ukarania za wypełnianie zadań.

Rola Inspektora Ochrony Danych

- Art. 39.1.a – informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO.
- Art. 39.1.b monitorowanie przestrzegania niniejszego rozporządzenia, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty.
- Art. 39.1.c udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35.
- Art. 39.1.d współpraca z organem nadzorczym.
- Art. 39.1.e pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem.
- Pełnienie punktu kontaktowego dla osób, których dane dotyczą.
- Prowadzenie rejestru czynności i rejestru kategorii czynności – zgodnie z art. 30 ust. 5 z prowadzenia rejestrów są zwolnione podmioty zatrudniające mniej niż 250 pracowników.

Rola Inspektora Ochrony Danych

- Funkcja Zastępcy Inspektora Ochrony Danych
  - wymagania,
  - zgłoszenie do PUODO.

Szacowanie ryzyka

Metody przeprowadzania analizy ryzyka w ochronie danych osobowych – wytyczne normy PN-ISO/IEC 27005

- Ryzyko jako **proces** opisany w normie 27005 – Szacowanie ryzyka w bezpieczeństwie informacji. Wspomniana norma koncentruje się na ryzykach występujących dla organizacji, jednak po właściwym zdefiniowaniu ryzyk i skutków dla osoby której dane dotyczą, opisane w niej postępowanie może być wykorzystane do szacowania ryzyka RODO
- Atrybuty bezpieczeństwa informacji:
  - poufność,
  - integralność,
  - dostępność,
  - rozliczalność,
  - autentyczność,
  - niezawodność.

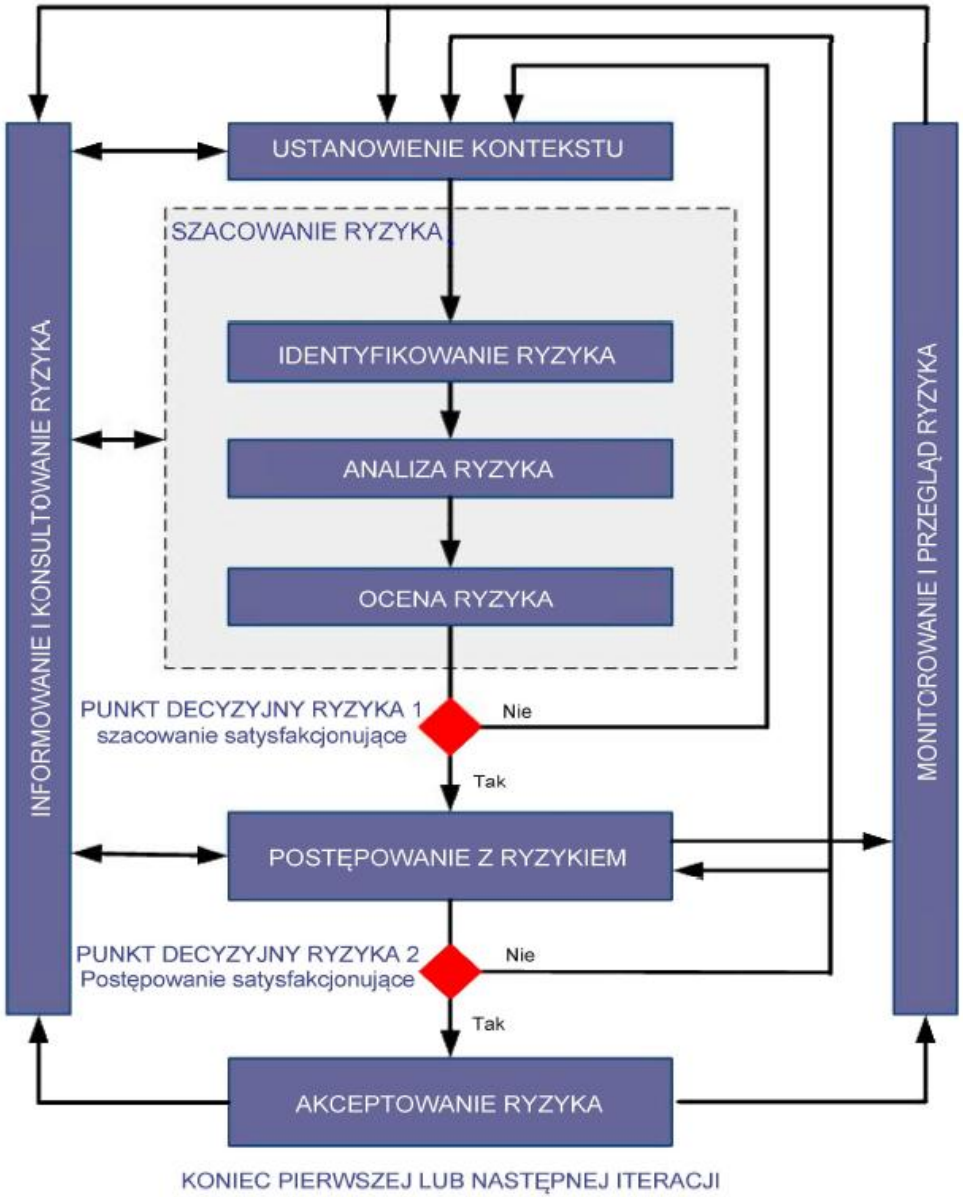
Wymagania RODO w zakresie szacowania ryzyka „hipotetycznego”

- Konieczność szacowania ryzyka wskazana w art. 24, 25 i 32 RODO.
- Celem szacowania ryzyka jest wyeliminowanie występujących zagrożeń i podatności poprzez wdrożenie adekwatnych środków technicznych opisanych w art. 32 RODO.

Wykorzystywanie norm ISO w ochronie danych osobowych oraz szacowaniu ryzyka

- Normy serii 29 100 - normy dotyczące ochrony danych identyfikujących osobę (PII).
- Normy serii 27 000 - normy dotyczące zarządzania bezpieczeństwem informacji.
- Normy serii 31 000 - zarządzanie ryzykiem – wytyczne.
- Normy serii 31 010 – zarządzanie ryzykiem - techniki oceny ryzyka.
- Powiązanie:
  - z normą 27001 - System zarządzania bezpieczeństwem informacji – wymagania,
  - z normą 29134 - Wytyczne dotyczące oceny skutków dla prywatności,
  - z normą 29151 - Praktyczne zasadny ochrony danych osobowych identyfikujących osobę, określa ona wytyczne dotyczące doboru zabezpieczeń.

Zarządzanie ryzykiem – proces



Źródła: Metodyka zarządzania ryzykiem cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów rządowych;

Szacowanie ryzyka – schemat postepowania wg normy PN-ISO/IEC 27005

- **Określ kontekst** – zakres i granice – jakiego procesu, danych, zasobów będzie dotyczyło szacowanie.
- **Zidentyfikuj aktywa** (Wartość aktywa dla organizacji może być inna aniżeli dla osoby której dane dotyczą):
  - aktywa podstawowe: procesy, działania biznesowe, informacje,
  - aktywa wspierające: systemy, sprzęt, oprogramowanie, sieć, personel, siedziba, struktura organizacyjna.
- **Zidentyfikuj posiadane zabezpieczenia.**
- **Zidentyfikuj ryzyka** (zagrożenia). Zagrożenie to niepożądane zdarzenie, którego zmaterializowanie się może doprowadzić do naruszenia poufności, integralności, dostępności danych.
- **Ustal plan postępowania z ryzykiem.**

Metody określania poziomu ryzyka

- **Metoda ilościowa**
  - bazują na wartościach monetarnych dla określenia wartości zasobu lub poniesionej straty,
  - bazująca na wartościach statystycznych w zakresie częstotliwości występowania zdarzenia,
  - daje wymierne wartości **jeśli** jesteśmy w stanie określić wartość zasobów oraz znamy dane statystyczne.
- **Metoda jakościowa**
  - korzysta z metod opisowych (małe, średnie, duże) zagrożeń, podatności, prawdopodobieństw i skutków,
  - bazuje na wiedzy i subiektywnej ocenie osoby dokonującej analizy,
  - uzyskany wynik jest najczęściej opisowy, można go przełożyć na wartości cyfrowe,
  - prostsze podejście,
  - umożliwia analizę zasobów trudno mierzalnych,
  - przykładem tej metody jest macierz ryzyka, ustalenie stopni oraz częstotliwości występowania ryzyka.

Przykłady

Macierz ze zdefiniowanymi wcześniej wartościami

	Poziom zagrożenia	NISKI			ŚREDNI			WYSOKI		
	Poziom podatności	N	Ś	W	N	Ś	W	N	Ś	W
Wartość zasobu	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Macierz ryzyka możliwego/niemożliwego do zaakceptowania

wartość szkód	0	1	2	3	4
wartość częstotliwości					
0	T	T	T	T	N
1	T	T	T	N	N
2	T	T	N	N	N
3	T	N	N	N	N
4	N	N	N	N	N

Metody określania poziomu ryzyka

- **Metoda oparta na rywalizacji:**
  - rywalizacja pomiędzy atakującym i broniącym się,
  - metoda skupia się na czynniku ludzkim: motywacji, umiejętności i skłonności do ryzyka.

$$R = \theta^2 \Psi 1/t^2 F$$

θ – poziom wiedzy atakującego

Ψ- stosunek skłonności do ryzyka strony atakującej do broniącej

$1/t$ – poziom nieznajomości systemu

F – stopień przekonania strony atakującej o sukcesie

Analiza ryzyka

Użyte skróty w analizie

P_z – prawdopodobieństwo wystąpienia zagrożenia

S_n – skutek naruszenia

R – ryzyko

Ocena prawdopodobieństwa wystąpienia zagrożenia P_z

Skala	Prawdopodobieństwo < P_z >	Opis	Częstotliwość wystąpienia
1	Pomijane	Prawdopodobieństwo wystąpienia zagrożenia jest bliskie zeru. Zagrożenie nie występowało w przeszłości. Nie wydaje się możliwe, by wybrane źródła ryzyka mogły doprowadzić do zmaterializowania się zagrożenia poprzez wykorzystanie zasobów (np.: kradzież wydruków składowanych w pomieszczeniu, do którego dostęp zabezpieczono czytnikiem kart i kodem dostępu).	1 x 50 lat
2	Ograniczone	Możliwość wystąpienia zagrożenia jest niewielkie. Wydaje się trudne, by wybrane źródła ryzyka doprowadziły do zmaterializowania się zagrożenia poprzez wykorzystanie zasobów (np.: kradzież wydruków składowanych w pomieszczeniu, do którego dostęp zabezpieczono czytnikiem kart).	1 x 10 lat
3	Poważne	Wystąpienie zagrożenia jest realne, waha się w granicach 50%. Zagrożenie występowało w przeszłości sporadycznie na przełomie ostatnich 5 lat. Wydaje się możliwe, że wybrane źródła ryzyka doprowadzą do zmaterializowania się zagrożenia poprzez wykorzystanie zasobów (np.: kradzież wydruków składowanych w pomieszczeniach biurowych podmiotu, do którego dostępu pilnuje osoba w recepcji).	1 x 5 lat
4	Maksymalne	Wydaje się oczywiste, że wybrane źródła ryzyka doprowadzą do zmaterializowania się zagrożenia poprzez wykorzystanie zasobów (np.: kradzież wydruków składowanych w holu ogólnym w siedzibie podmiotu).	1 x rok

Określenie skutków naruszenia, w tym praw i wolności osób fizycznych – waga szkody S_n

Skala	Skutek $< S_n >$	Opis dla osób fizycznych	
1	Pomijany	Nie ma praktycznie żadnego wpływu na powstanie uszczerbku fizycznego, szkód majątkowych i niemajątkowych u osob fizycznych.	Nikły wpływ na funkcjonowanie. Nie spowoduje strat w zakresie ważnych zasobów.
2	Ograniczony	Może spowodować powstanie uszczerbku fizycznego, szkód majątkowych lub niemajątkowych, u osób fizycznych.	Może zakłócić realizację niektórych celów, zaszkodzić interesom i reputacji oraz finansom
3	Poważny	Może spowodować powstanie dużego uszczerbku fizycznego, szkody niemajątkowe lub majątkowe, takie jak: utrata kontroli nad swoimi danymi, ograniczenie praw, dyskryminacja, kradzież, sfałszowanie tożsamości, strata finansowa, może spowodować powstanie wysokiego naruszenia praw i wolności osób fizycznych,	Może spowodować straty dla ważnych zasobów, zakłucić realizację funkcjonowania instytucji i wstrzymac realizację ciągłości funkcjonowania procesów oraz zaszkodzić w dużym stopniu reputacji oraz finansom
4	Maksymalny	Może spowodować powstanie bardzo dużego uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych takich jak: utrata kontroli nad swoimi danymi, pozbawienie praw, dyskryminacja, sfałszowanie tożsamości, strata finansowa, znaczna szkoda gospodarcza oraz społeczna.	Może spowodować największe możliwe straty dla ważnych zasobów. Skutek może zakłucić realizację ciągłości funkcjonowania całej instytucji, wstrzymać realizację ciągłości funkcjonowania wszystkich procesów i zaszkodzić w bardzo dużym stopniu reputacji oraz finansom

Macierz ryzyka oraz postępowanie z ryzykiem

Macierz ryzyka

$R = P_z \times S_n$

Prawdopodobieństwo P_z		Skutkek (S_n)			
		1	**2**	**3**	**4**
	1	1	2	3	4
	2	2	4	6	8
	3	3	6	9	12
	4	4	8	12	16

Postępowanie z ryzykiem

Wartości	Skala	Opis
Pomijane	1 =< R <= 3	Brak reakcji na ryzyko lub o jego tolerowanie; zarządzający akceptuje ryzyko (ryzyko nieznaczne); dana działalność niesie za sobą potencjalnie wyższą wartość dodaną niż koszt stosowanych środków ochrony; powstało ryzyko rezydualne (pozostałe), którego nie można całkowicie wyeliminować środkami ochrony; tworzy się plany awaryjne, które stanowią zabezpieczenie w momencie wzrostu ryzyka, ryzyko jest monitorowane
Ograniczone	4 =< R <= 6	Zapobieganie wystąpieniu ryzyka lub zmniejszenie jego skutków poprzez zastosowanie takich mechanizmów jak: systematyczna ocena i monitorowanie ryzyka, stosowanie technicznych i organizacyjnych środków ochrony zasobów, wdrożenie procedur kontrolnych, szkolenie personelu, wprowadzenie systemów jakości, ocena dostawców usług zewnętrznych, zabezpieczenia prawne wykonania umów i inne mechanizmy zapobiegawcze, nakazowe, korygujące, wykrywające
Poważne	8 =< R <= 9	Należy zdywersyfikować ryzyka poprzez rozproszenie ryzyka, np. outsourcing obsługi działań, w których brakuje kompetencji w instytucji, a także: zmniejszenie koncentracji ryzyka IT związanego z kluczowymi dostawcami sprzętu, zabezpieczeń, usług serwisowych itp. Kolejnym rozwiązaniem może być transfer ryzyka poprzez przeniesienie na inne podmioty poprzez np. ubezpieczenie: od zdarzeń losowych, baz danych, sprzętu informatycznego, projektu.
Maksymalne	12 =< R <= 16	Jeżeli zarządzający nie potrafi obniżyć poziomu ryzyka należy rozważyć rezygnację z procesu lub redefinicję procesu w taki sposób, aby wyeliminować lub zmniejszyć ryzyko nieodzowne w działalności, metodami organizacyjnymi (np. podział uprawnień użytkowników systemów informatycznych), lub metodami technicznymi (np. zakup dobrej jakości sprzętu i systemów, zabezpieczenie techniczne serwerowi), lub rezygnacja z prowadzenia projektu narażonego na duże ryzyko niepowodzenia

Przykłady zidentyfikowanych aktywów w procesie szacowania ryzyka

Analiza i ocena aktywów

W ramach procesów przetwarzania danych wyróżniamy następujące rodzaje aktywów podstawowych, wspierających procesy przetwarzania lub ich grup:

Aktywa:	Części składowe zdefiniowanych aktywów
Aktywa podstawowe	
Zbiory wykorzystywane w procesie przetwarzana danych osób fizycznych	**Dane osobowe**
Pracownicy biorący udział w procesie przetwarzana danych	- Kandydatów do pracy
	- Pracowników
	- Osób zatrudnionych w ramach unmów cywilno-prawnych
	- Dostawców i kontrahentów oraz pracowników ich reprezentujących
	- Podpiecznych MOPS
	- Stażystów i wolontariuszy i praktykantów
	- Oferentów w ramach zamówień publicznych
	- Osób składających skargi i wnioski
	- Osób wnioskujących o dostęp do informacji publicznej
	- Osób korespondujących
	- Osób korzystających ze strony www oraz mediów społecznościowych
	- Dane osobowe przechwywane w archiwum zakładowym

Przykłady zidentyfikowanych aktywów w procesie szacowania ryzyka

Aktywa wspierające	
Posiadane dokumentacja, procedury d. przetwarzania	**Czynnik ludzki**
	- Regulaminy, instrukcjie, procedury
	- Upoważnienia,
	- Umowy powierzenia i udostępnienia
	- Umowy serwisowe
	- Szkolenia z zakresu ochrony danych
	- Umowy z dostawcami usług
	- Umowy z firmami współpracującymi
	- Rozliczalność w zakresie odpowiedzialności oraz w zakresie praw dostępu
Sprzęt służący do przetwarzania danych	**Sprzęt**
	- Serwery
	- Macierze
	- Stacje robocze, laptopy
	- Urządzenia aktywne sieci komputerowej (switche, przełączniki, access pointy)
	- Urządzenia brzegowe
	- Zasilacze awaryjne
	- Smartfony, tablety
	- Skanery, drukarki, aparaty fotograficzne, urządzenia wielofunkcyjne, kamery
	- Urządzenia przenośne (Pendrive, płyty CD, DVD, karty pamięci, dyski)

Przykłady zidentyfikowanych aktywów w procesie szacowania ryzyka

	- Pomieszczenia i sprzęt służący do przechowywania dokumentacji papierowej
Środowisko IT służące do przetwarzania danych	**Infrastruktura IT**
	- Okablowanie strukturalne
	- Sieć wewnętrzna
	- Zabezpieczenia na styku z siacią Internet
	- Kanały łączności
	- systemy wentylacji i klimatyzacji
	- Systemy kontroli dostępu
	- Systemy PPOŻ
	- Systemy powiadamiania
	- Systemy monitoringu środowiska
	- Systemy monitoringu SSWIN
	- Systemy CCTV

Przykłady zidentyfikowanych aktywów w procesie szacowania ryzyka

Wykorzystywane oprogramowanie	Oprogramowanie
	- Oprogramowanie serwerowe
	- Systemy operacyjne na stacjach końcowych
	- Systemy operacyjne w telefonach, tabletach
	- Oprogramowanie klienckie służące do przetwarzania danych
	- Oprogramowanie antywirusowe
	- Oprogramowanie monitorujące
	- Oprogramowanie do backupu
	- Oprogramowanie układowe urządzeń
	- Oprogramowanie zabezpieczające (szyfrowanie, anonimizacja, pseudonimizacja)

Przykłady zidentyfikowanych aktywów w procesie szacowania ryzyka

Infrastruktura techniczna	Siedziba/miejsce przetwarzania danych
	- Zabezpieczenia zewnętrzne - kraty, rolety i drzwi antywłamaniowe
	- Ogrodzony teren
	- KD
	- PPOŻ
	- CCTV
	- SSWIN
	- Ochrona fizyczna
	- Lokalizacja przetwarzania przy pracy zdalnej

Przykłady zidentyfikowanych zabezpieczeń w procesie szacowania ryzyka

- Zabezpieczenia wpływają na prawdopodobieństwo i skutek zmaterializowania się zagrożenia.
- Istnieje możliwość korzystania z wykazu zabezpieczeń zawartego w normie 27002. W przypadku zabezpieczeń danych osobowych właściwsza jest norma 29151, która jednak w większości zawiera odniesienia do normy 27002

Kategoria zabezpieczenia		Występuje
Zabezpieczenia prawne (umowy, oświadczenia, zobowiązania)	Umowy powierzenia	Tak
	Umowy z firmami świadczącymi usługi wsparcia	Tak
	Umowy najmu, porozumienia z właścicielem	Nie dotyczy
	Upoważnienia do przetwarzania danych	Tak
	Oświadczenia o zachowaniu w poufności	Tak
Zabezpieczenia organizacyjne (procedury, polityki, szkolenia, audyty, testy)	Procedury dotyczące przetwarzania	Tak
	Procedury pracy zdalnej	Tak/Nie
	Instrukcja postepowania w sytuacji naruszenia danych osobowych	Tak
	Procedura realizacji praw podmiotów danych	Tak
	Klauzule informacyjne - spełninie obowiązku informacyjnego	Tak
	Polityka kluczy	Tak
	Procedury użytkowania systemu komputerowego i poczty email	Tak
	Szkolenia personelu z zakresu przetwarzania danych, procedury	Tak
	Zarządzanie uprawnieniami	Tak
	Ograniczony zakres uprawnień użytkowników	Tak
	Kontrola rejestrowania działań użytkowników	Tak
	Polityka backupu oraz kontrola poprawności wykonania kopii zapasowych	Tak
	Okresowe przeglądy sprzętu i konfiguracji	Tak
	Aktualizacje systemów	Tak
	Audyty, kontrole, sprawdzenia	Tak
	Rozliczalność - domena, indywidualne konta	Tak

	Inwentaryzacja sprzętu	Tak
	Monitorowanie zmian w przepisach prawa	Tak
	Nadzór nad ochroną danych	Tak
	Outsourcing	Tak
	Procedura niszczenia danych	Tak
	Procedura przywracania danych	Tak
	Procedura postepowania z nośnikami i sprzętem	Tak
	Procedura korzystania z Internetu	Tak
	Oprogramowanie antywirusowe	Tak
	Kopie zapasowe	Tak
	Ochrona kryptograficzna transmisji	Tak
	Pseudonimizacja danych	Tak
	Filtrowanie i kontrola ruchu sieciowego	Tak
	Wykrywanie i blokowanie naruszeń bezpieczeństwa	Tak
	Podtrzymanie zasilania	Tak
	Środowisko testowe - wirtualizacja	Nie dotyczy
	Odpowiednio skonfigurowany dostęp zdalny	Tak

Zabezpieczenie techniczne	Odpowiednie zabezpieczenie dokumentów papierowych oraz pomieszczeń	**Tak**
	Przechowywanie kopii zapasowych poza siedzibą lub w innym pomieszczeniu	**Tak**
	Redundancja	**Tak**
	Monitorowanie pracy urządzeń	**Tak**
	Monitoring środowiska	**Tak**
	Szyfrowanie urządzeń przenośnych	**Tak**
	Szyfrowanie transmisji	**Tak**
	Ochrona przed zagrożeniami naturalnymi (PPOŻ)	**Tak**
	System CCTV	**Nie dotyczy**
	System SSWIN	**Tak**
	System KD	**Tak**
	Klimatyzacja/wentylacja	**Tak**
Zabezpieczenia fizyczne	Ochrana fizyczna budynku	**Nie dotyczy**
	Ogrodzony teren	**Nie dotyczy**
	Kraty w oknach	**Tak**
	Drzwi antywłamaniowe	**Tak**
	Rolety antywłamaniowe	**Nie dotyczy**
	Drzwi zamykane na klucz	**Tak**
	Dokumenty zamykane na klucz	**Tak**

Przykłady występujących zagrożeń w procesie szacowania ryzyka

- Analiza zagrożeń.
- Analiza podatności.
- **Szacowanie ryzyka:**
  - ocena prawdopodobieństwa zmaterializowania się zagrożenia,
  - ocena skutków dla osoby fizycznej (organizacji) zmaterializowania się zagrożenia.

Aktyw	Przykładowe zagrożenia	Podatność	Prawdopodobieństwo <P> <1 - 4>	Skutek <S> <1 - 4>	Ryzyko dla osoby <P x S> <1 - 16>	Skutek <S^a> <1 - 4>	Ryzyko dla Administratora <P x S^a> <1 - 16>
Zbiory	Uzyskanie przez osobę nieuprawnioną dostępu do danych	Brak oprogramowania zabezpieczającego.	1	2	2	2	2
	Utrata danych	Źle skonfigurowane urządzenia sieciowe i brzegowe	1	1	1	1	1
	Brak możliwości odtworzenia danych	Brak backupu danych	1	1	1	1	1
	Pożar	Nieprzestrzeganie zasad PPOŻ	1	1	1	1	1
	Utrata danych	Brak monitorowania działania sprzętu	1	1	1	2	2
	Utrata danych	Brak umów powierzenia danych	1	2	2	3	3
	Umyślne lub nieumyślne udostępnienie danych osobie niepowołanej	Błędy i pomyłki użytkowników	2	2	4	3	6
	Zniszczenie danych	Zaniedbania	1	1	1	2	2
	Umyślne lub nieumyślne udostępnienie danych osobie niepowołanej	Niestosowanie się do procedur bezpieczeństwa na stanowisku pracy	2	2	4	3	6
	Umyślne lub nieumyślne udostępnienie danych osobie niepowołanej	Brak reguły czystego biurka i ekranu	2	2	4	3	6
	Umyślne lub nieumyślne udostępnienie danych osobie niepowołanej	Brak blokowania ekranu przy opuszczaniu stanowiska pracy	2	2	4	3	6
	Umyślne lub nieumyślne udostępnienie danych osobie niepowołanej	Brak procedur nadzoru, oraz osób odpowiedzialnych	2	2	4	3	6
	Utrata danych	Brak osób odpowiedzialnych za systemy, procesy, zasoby	1	1	1	2	2
	Umyślne lub nieumyślne udostępnienie danych osobie niepowołanej	Niewłaściwy przydział uprawnień dostępu	1	2	2	3	3
	Brak kontroli nad danymi	Bark nadzoru nad firmami zewnętrznymi	1	2	2	3	3
	Utrata danych	Nieodpowiednie lub brak zabezpieczenia wyników swojej pracy	1	1	1	2	2
	Utrata danych - Phishing	Wejście na podrobioną stronę	1	1	1	2	2

Czynnik ludzki	Utrata danych - wirus, ransomeware	Przeglądanie niewłaściwych stron www, otwieranie załączników z maili	2	2	4	2	4
	Utrata danych	Wynoszenie dokumentów lub nośników bez wiedzy Administratora	1	2	2	3	3
	Utrata danych - socjotechnika	Wyłudzenie danych	2	2	4	3	6
	Utrata danych - włamanie, hacking, cracking	Źle skonfigurowane urządzenia sieciowe i brzegowe	1	2	2	3	3
	Utrata i brak możiwości odtworzenia danych	Przechowywanie kopii w miejscu wytwarzania lub ich brak	1	1	1	2	2
	Naruszenie dostępności personelu	Nieobecność personelu	1	1	1	2	2
	Błąd użytkowania	Niepoprawne użycie oprogramowania lub sprzętu	1	1	1	2	2
	Błąd użytkowania	Brak świadomości w zakresie bezpieczeństwa	2	1	2	2	4
	Nielegalne przetwarzanie danych	Brak mechanizmów monitorowania	1	2	2	3	3
	Nielegalne przetwarzanie danych	Praca personelu zewnętrznego lub sprzątającego bez nadzoru	1	2	2	3	3
	Niespełnienie obowiązku informacyjnego	Barak osób odpowiedzialnych	2	2	4	3	6
	Brak realizcji praw osób	Barak osób odpowiedzialnych	1	2	2	3	3
	Zbyt długi czas przechowywania danych	Nieusuwanie danych po okresie retencji	1	2	2	3	3
	Zbieranie danych nadmiarowych	Nieprzestrzeganie zasady minimalizacji danych	1	2	2	3	3
	Brak respektowania przepisów prawa	Zmieniające się przepisy	1	1	1	2	2
	Zagubienie / utrata nośników z danymi	Nie przestrzeganie procedur	1	2	2	3	3
	Ataki man-in-the-middle	Logowanie do niezaufanych sieci	1	2	2	2	2
	Brak odpowiedniej dokumentacji zarządzania systemami IT	Odejście pracownika z pracy	1	1	1	2	2
	Brak weryfikacji danych	Wykorzystanie niezweryfikowanych danych	1	2	2	3	3
	Zagrożenia prawne	Nieinformowanie Administratora o naruszeniach/incydentach	1	2	2	3	3

	Naruszenie bezpieczeństwa informacji	Odtworzenie danych z wyrzuconych nośników	1	2	2	3	3
	Nieautoryzowane działania	Użycie urządzeń, kopiowanie oprogramowania	1	2	2	3	3
	Nadużycie praw	Brak formalnej procedury rejestrowania i wyrejestrowywania użytkownika	1	2	2	3	3
	Naruszenie zdolności utrzymania systemu informatycznego	Nieodpowiedni czas reakcji utrzymania serwisowego	1	1	1	2	2
	Błąd użytkownika	Brak procedur korzystania z poczty oraz komputera	2	2	4	3	6
	Dostęp osób nieupoważnionych	Brak umów lub niewłasciwe zapisy w umowię z najemcą	0	1	0	2	0
	Dostęp osób nieupoważnionych	Brak upoważnień do przetwazrania danych	1	2	2	3	3
	Dostęp osób nieupoważnionych	Korzystanie z prywatnych telefonów	2	2	4	3	6
	Dostęp osób nieupoważnionych	Przetwarzanie danych w domu	2	2	4	3	6
	Kradzież użądzenia	Brak nadzoru nad aktywami znajdującymi się poza siedzibą	2	2	4	3	6
	Kradzież, nośników dokumentów	Niestosowanie się do polityki czystego biurka lub jej brak	2	2	4	3	6
Sprzęt	Awaria, uszkodzenie, niedostepność serwera	Brak okresowych przeglądów oraz monitorowania pracy serwerów	1	1	1	2	2
	Awaria, uszkodzenie, niedostepność serwera	Przegrzanie	1	1	1	2	2
	Awaria, uszkodzenie, niedostepność serwera	Awaria zasilania - brak potrzymania zasilania	1	1	1	2	2
	Awaria, uszkodzenie, niedostepność macierzy	Brak okresowych przeglądów oraz monitorowania pracy macierzy	1	1	1	2	2
	Awaria, uszkodzenie, niedostepność macierzy	Przegrzanie, uszkodzenie dysku	1	1	1	2	2
	Awaria, uszkodzenie, niedostepność macierzy	Uszkodzenie urządzenia	1	1	1	2	2
	Awaria, uszkodzenie, niedostepność macierzy	Awaria zasilania - brak potrzymania zasilania	1	1	1	2	2
	Awaria, uszkodzenie, niedostepność stacji roboczej	Zanieczyszczenie, utrata zasilania, przepięcie	1	1	1	2	2

	Awaria, uszkodzenie, niedostepność urządzeń aktywnych	Uszkodzenie, awaria zasilania	1	1	1	2	2
	Awaria, uszkodzenie, niedostepność urządzenia brzegowego	Uszkodzenie, błedna konfiguracja, zhakowanie	1	1	1	2	2
	Awaria, uszkodzenie, niedostepność zasilacza awaryjnego	Udzkodzenie	1	1	1	1	1
	Korzystanie z prywatnych komputerów podczas pracy zdalnej	Praca zdalna	2	2	4	2	4
	Awaria, uszkodzenie wentylacji, klimatyzacji	Uszkodzenie	1	1	1	2	2
Środowisko IT	Naruszenie zdolności utrzymania systemu informatycznego	Niewystarczające utrzymanie/błędna instalacja nośników pamięci	1	1	1	2	2
	Zniszczenie urządzeń lub nośników	Brak planów okresowej wymiany	1	1	1	2	2
	Pył, korozja, wychłodzenie	Wrażliwość na wilgoć, pył, zanieczyszczenie	1	1	1	2	2
	Promieniowanie elektromagnetyczne	Wrażliwość na promieniowanie elektromagnetyczne	1	1	1	2	2
	Błąd użytkowania	Brak skutecznej kontroli zmian konfiguracji	1	1	1	2	2
	Utrata zasilania lub przepięcia	Wrażliwość na zmiany napięcia zasilania	1	1	1	2	2
	Zjawiska pogodowe	Wrażliwość na zmiany temperatury	1	1	1	2	2
	Kradzież nośników lub dokumentów	Niezabezpieczone urządzenia do przechowywania danych	1	2	2	3	3
	Kradzież nośników lub dokumentów	Brak staranności przy pozbywaniu się nośników	1	2	2	3	3
	Kradzież nośników lub dokumentów	Niekontrolowane kopiowanie	1	2	2	3	3
	Ataki na sprzęt	Niewłaściwa konfigutacja sprzetu,	1	2	2	3	3
	Przeciążenie systemu	Zła konfiguracja, awaria	1	1	1	2	2
	Podsłuch	Niezabezpieczone linie telekomunikacyjne	1	2	2	3	3
	Podsłuch	Niechroniony wrażliwy ruch	1	2	2	3	3
	Awaria urządzenia telekomunikacyjnego	Złe łączenie kabli	1	1	1	2	2

	Awaria urządzenia telekomunikacyjnego	Pojedynczy punkt uszkodzenia	1	1	1	2	2
	Fałszowanie praw	Brak identyfikacji i uwierzytelnienia nadawcy i odbiorcy	1	2	2	3	3
	Szpiegostwo zdalne	Niebezpieczna architektura sieciowa	1	2	2	3	3
	Szpiegostwo zdalne	Przesyłanie hasła w jawnej postaci	1	2	2	3	3
	Nieautoryzowane użycie urządzeń	Niezabezpieczone połączenia z siecią publiczną	1	2	2	3	3
	Brak dostępu do środowiska	Odejście z pracy administratora	1	1	1	2	2
	Ataki na sprzęt	Brak aktualizacji oprogramowania układowego	1	2	2	3	3
Oprogramowanie	Włamanie do systemu	Brak aktualizacji oprogramowania	1	2	2	3	3
	Zainfekowanie systemu złośliwym oprogramowaniem	Nieaktualne lub brak oprogramowania antywirusowego	1	2	2	3	3
	Uszkodzenie bazy danych	Nieaktualne oprogramowanie, brak oprogramowania zabezpieczającego	1	1	1	3	3
	Utrata danych	Brak informacji o awariach	1	1	1	3	3
	Naruszenie poufności danych	Brak lub niewłasciwe oprogramowanie szyfrujące	1	2	2	3	3
	Brak możliwości odtworzenia danych w przypadku awarii	Brak lub niewasciwe oprogramowanie do backupu	1	1	1	2	2
	Brak kontroli na oprogramwaniem	Korzystanie z prywatnych komputerów podczas pracy zdalnej	2	2	4	3	6
	Kradzież danych	Niewłaściwe lub brak szyfrowania urządzeń przenośnych	1	2	2	3	3
Siedziba	Kradzież sprzętu i danych	Brak odpowiednich zabezpieczeń fizycznych lub/i osobowych	1	2	2	3	3
	Kradzież sprzętu i danych	Brak procedur otwierania/zamykania	0	2	0	3	0
	Kradzież sprzętu i danych	Zła obsługa i proces nadawania uprawnień,	1	2	2	3	3
	Kradzież sprzętu i danych	Brak kontroli działania systemów	1	2	2	3	3
		Średnie ryzyko w procesie	**1,15**	**1,56**	**1,85**	**2,49**	**2,92**

Przykłady wdrożonych środków mających na celu obniżenie poziomu ryzyka w procesie szacowania ryzyka

Aktyw	Środki ograniczajce ryzyko	Występuje Tak/Nie/ Nie dotyczy	Do wdrożenia	Dział	Termin wdrożenia	Osoba odpowiedzialna
Zbiory	Oprogramowanie antywirusowe, aktualizacja oprogramowania	Tak				
	Monitorowanie pracy urządzeń, aktualizacja oprogramowania	Tak				
	Backup danych oraz kontrola poprawności wykonania	Tak				
	Procedury, gaśnice, system PPOŻ	Tak				
	Monitoring środowiska i urządzeń	Tak				
	Umowy powierzenia danych	Tak				
	Szkolenia, Procedury, Kontrola	Tak				
	Jasne i przejrzyste procedury	Tak				
	Procedury organizacyjne, kontrola, monitorowanie	Tak				
	Szkolenia, procedury	Tak				
	Szkolenia, procedury	Tak				
	Kontrola, procedury organizacyjne	Tak				
	Procedury organizacyjne	Tak				
	Procedury organizacyjne, kontrola, monitorowanie	Tak				
	Umowy powierzenia danych	Tak				
	Szkolenia, procedury	Tak				
	Szkolenia, procedury	Tak				

Czynnik ludzki	Szkolenia, procedury, zasady korzystania z sieci internet	Tak				
	Szkolenia, procedury, regulaminy	Tak				
	Szkolenia, procedury	Tak				
	Audyty bezpieczeństwa systemów, monitorowanie pracy	Tak				
	Redundancja kopii, przechowywanie w innej lokalizacji	Tak				
	Procedury organizacyjne dotyczące zastępstw	Tak				
	Ograniszony zakres uprawnień, szkolenia, rozliczalność	Tak				
	Szkolenia w zakresie ochrony danych	Tak				
	Kontrola rejestrowania działań użytkowników, rozliczalność	Tak				
	Procedury organizacyjne dotyczące firm zewnętrznych	Tak				
	Spełninie obowiązku informacyjne - osoby odpowiedzialne za ich realizację	Tak				
	Procedura realizacji praw podmiotu danych - osoby odpowiedzialne	Tak				
	Audyty, kontrole, sprawdzenia	Tak				
	Audyty, kontrole, sprawdzenia	Tak				
	Śledzenie zmian, wyznaczenie osób odpowiedzialnych	Tak				
	Szkolenia, procedury, szyfrowanie urządzeń przenośnych, zamykanie pomieszczeń	Tak				
	Procedury, szkolenia	Tak				
	Aktualizacja dokumentacji, zdeponowane hasła ASI	Tak				
	Wdrożone procedury	Tak				
	Szkolenia, instrukcja postępowania w przypadku naruszenia	Tak				

	Procedura postepowania z nośnikami i sprzętem	Tak				
	Ograniczony zakres uprawnień, rozliczalność	Tak				
	Rozliczalność - domena	Tak				
	Zapisy w umowach na świadczenie usług	Tak				
	Procedura korzystania z poczty i komputera	Tak				
	Umowa z wynajmującym	Nie dotyczy				
	Wydane upoważnienia oraz oświadczenia o zachowaniu w poufności	Tak				
	Procedura dotycząca zasad korzystania	Tak				
	Procedura pracy zdalnej	Tak/Nie	Procedury pracy zdalnej			
	Inwentaryzcja sprzetu, szyfrowanie	Tak				
	Procedury, szkolenia, odpowiednie zabezpieczenie dokumentacji papierowej i archiwum, serwerowni	Tak				
Sprzęt	Przeglady systemów, monitorowanie pracy, wgrywanie aktualizacji, redundancja	Tak				
	Wentylacja. Klimatyzacja	Tak				
	Podtrzymanie zasilania, listnwy filtrujące	Tak				
	Przeglady systemów, monitorowanie pracy, wgrywanie aktualizacji, redundancja	Tak				
	Wentylacja, klimatyzacja	Tak				
	RAID - redundancja	Tak				
	Podtrzymanie zasilania, listnwy filtrujące	Tak				
	Redundancja, przeglądy, podtrzymanie zasilania	Tak				

	Redundancja, przeglądy, podtrzymanie zasilania, monitorowanie	Tak				
	Redundancja, przeglądy, podtrzymanie zasilania, aktualizacja oprogramowania, monitorowanie	Tak				
	Redundancja, przeglądy	Tak				
	Porozumienie z pracownikiem - dostosowanie sprzetu do wymagań Administratora	Tak/Nie	Procedury pracy zdalnej			
	Przeglądy, redundancja	Tak				
Środowisko IT	Okresowe przeglądy, monitorowanie pracy	Tak				
	Okresowe przeglądy, redundancja, RAID, backup	Tak				
	Okresowe przeglądy, czyszczenie	Tak				
	Zabezpieczeniia organizacyjne	Tak				
	Środowisko testowe, wirtualizacja	Tak				
	Podtrzymanie zasilania, listnwy filtrujące	Tak				
	Klimatyzacja, wentylacja, monitorowanie środowiska (wilgotność, zalanie, dym)	Tak				
	KD, CCTV, Ochrona fizyczna obiektu, polityka kluczy	Tak				
	Procedura niszczenia, utylizacji nośników	Tak				
	Ograniczony zakres uprawnień, rozliczalność	Tak				
	Filtrowanie i kontrola ruchu sieciowego, Wykrywanie i blokowanie naruszeń bezp.	Tak				
	Monitorowanie pracy systemu	Tak				
	Szyfrowanie transmisji	Tak				
	Ochrona kryptograficzna transmisji	Tak				
	Ograniczony zakres uprawnień, rozliczalność	Tak				

Działania korygujące poziom ryzyka

Działania korudujące poziom ryzyka		Działanie
Akceptacja - zachowanie ryzyka	Godzimy się z możliwością wystąpienia incydentu, jego skutki są ekonomicznie akceptowalne a koszt wdrożenia zabezpieczeń przewyższa wartość ewentualnych strat	A
Minimalizacja - modyfikowanie ryzyka	Wdrożenie rozwiązań, które zapobiegają wystąpieniu ryzyka lub zmniejszających poziom ryzyka (techniczne lub operacyjne środki zaradcze)	M
Unikanie ryzyka	Unikanie i eliminacja działań powodujących występowanie ryzyka	U
Przeniesienie - dzielenie ryzyka	Przekazywanie ryzyka innemu podmiotowi (zewnętrzny dostawca, podwykonawca)	P

Podsumowanie wraz zaleceniami dotyczącymi postępowania z ryzykiem

Podsumowanie

Analiza ryzyka

	Średnie ryzyko w poszczególnych procesach	Dla osoby fizycznej	Dla organiacji	Działanie
1.	Proces przetwarzania danych w związku z rekrutacją pracowników	1,85	2,92	A
2.	Proces przetwarzania danych w związku zatrudnieniem pracowników - umowy o pracę,	3,54	3,64	MUP
3.	Proces przetwarzania danych w związku z umowami cywilno-prawnymi z osobami fizycznymi nieprowadzącymi działalności gospodarczej - zlecenie,	3,48	3,58	MUP
4.	Proces przetwarzania danych w związku umowami cywilno-prawnymi z osobami fizycznymi prowadzącymi działalność gospodarczą,	2,07	3,51	A
5.	Proces przetwarzania danych pracowników reprezentujących kontrahentów oraz osób fizycznych reprezentujących podmioty prawne	1,87	3,51	A
6.	Proces przetwarzania danych stażystów, praktykantów i wolontariuszy,	3,42	3,56	MUP
7.	Proces przetwarzania danych w ramach ZFŚS,	2,07	3,51	A

Szacowanie ryzyka rzeczywistego na przykładzie ENISY - przykład

Konsekwencje niewłaściwego stosowania przepisów RODO w programie Fundusze Europejskie dla Łódzkiego 2021-2027

Ogólne warunki nakładania administracyjnych kar pieniężnych i ich zależność od świadomości oraz postawy personelu

- Każdy organ nadzorczy zapewnia, by stosowane na mocy niniejszego artykułu za naruszenia niniejszego rozporządzenia administracyjne kary pieniężne były w każdym indywidualnym przypadku skuteczne, proporcjonalne i odstraszające.
- Administracyjne kary pieniężne nakłada się, zależnie od okoliczności każdego indywidualnego przypadku. Decydując, czy nałożyć administracyjną karę pieniężną oraz ustalając jej wysokość, zwraca się w każdym indywidualnym przypadku należytą uwagę na:

- charakter, wagę i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób, których dane dotyczą, oraz rozmiaru poniesionej przez nie szkody,
- umyślny lub nieumyślny charakter naruszenia

Ogólne warunki nakładania administracyjnych kar pieniężnych i ich zależność od świadomości oraz postawy personelu

- działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody,
- stopień odpowiedzialności administratora lub podmiotu przetwarzającego,
- wszelkie stosowne wcześniejsze naruszenia ze strony administratora lub podmiotu przetwarzającego,
- stopień współpracy z organem nadzorczym,
- kategorie danych osobowych, których dotyczyło naruszenie,
- sposób, w jaki organ nadzorczy dowiedział się o naruszeniu.

Pamiętaj!!!

- **Przetwarzając dane z upoważnienia Administratora to od Twojej świadomości z zakresu przetwarzania danych i cyberbezpieczeństwa oraz od Twojego zaangażowania zależy bezpieczeństwo danych osobowych. Ponad 77% naruszeń bezpieczeństwa jest spowodowane przez pracowników**

- **Zawsze reaguj na zaobserwowane nieprawidłowości w obszarze przetwarzania.**

- **Nie bój się zwracać uwagi osobom których niewłaściwe postępowanie może przyczynić się do wystąpienia naruszenia ochrony danych.**

- **Jeżeli sam popełnisz błąd pamiętaj, że niezgłoszenie tego do Inspektora Ochrony Danych lub Administratora może mieć dla Ciebie niewspółmiernie poważniejsze konsekwencje aniżeli sytuacja, w której przyznasz się do popełnionego błędu.**

- **Zawsze reaguj na żądania osób których dane dotyczą.**

- **Pamiętaj o bezwzględnej konieczności identyfikacji osoby przed udzieleniem jej informacji – to że osoba podaje się za pacjenta, pracownika instytucji (ZUS, Policja, NFZ, Sanepid) nie znaczy że nim faktycznie jest, nawet jeżeli numer z którego dzwoni jest numerem wspomnianej instytucji.**

RODO to nie fikcja – nałożone kary w Polsce

Lp+F	Kwota (PLN)	Kwota (EUR)	Data	Nazwa i określenie podmiotu	Powód
1	1 500,00	350,47	2023	Wspólnota mieszkaniowa	Brak zgłoszenie na ruszenia Brak umowy powierzenia danych Brak weryfikacji podmiotu przetwarzającego
2	30 000,00	7 009,35	2023	Sąd Rejonowy Szczecin Centrum	Brak wdrożenia adekwatnych środków technicznych i organizacyjnych - zgubienie trzech urządzeń (niezaszyfrowanych) pendrive z danymi
3	6 854,00	1 601,40	2022	Pan R.G.	Brak współpracy z UODO - nieodpowiadanie na wezwania UODO
4	2 285,00	533,88	2022	Pełnomocnik Inicjatorów Referendum Gminnego	Brak współpracy z UODO - nieodpowiadanie na wezwania UODO
5	32 000,00	7 476,64	2022	TIMSHEL Spółkę z ograniczoną odpowiedzialnością	Zgłoszenie naruszenia bez załącznika a następnie nieodpowiadanie na wezwania UODO
6	1 600 000,00	373 831,78	2022	P4 (Virgin Mobile)	Brak wdrożenia adekwatnych środków technicznych i organizacyjnych
7	250 000,00	58 411,21	2022	P4	Niezgłoszenie naruszenia ochrony danych oraz niepowiadomienie osób których dane dotyczą w ustawowym terminie
8	8 000,00	1 869,16	2022	Wójta gminy Dobrzyniewo Duże	Brak wdrożenia adekwatnych środków technicznych i organizacyjnych - niezaszyfrowany laptop
9	2 500,00	584,11	2022	Sułkowicki Ośrodek Kultury	Brak zawartej umowy powierzenia danych oraz weryfikacji podmiotu przetwarzającego
10	10 000,00	2 336,45	2022	Główny Geodeta Kraju z siedzibą w Warszawie	Niezgłoszenie naruszenia do Prezesa UODO oraz brak poinformowania osoby której dane zostały ujawnione
11	60 000,00	14 018,69	2022	Główny Geodeta Kraju z siedzibą w Warszawie	Niezgłoszenie naruszenia do UODO - przez ponad 48 godzin w systemie geoportal widoczne były numey ksiąg wieczystych
12	10 000,00	2 336,45	2022	Stołeczny Ośrodek dla Osób Nietrzeźwych	Przetwarzanie danych bez podstawy prawnej - nagrywanie obrazu i dźwięku w systemie monitoringu
13	16 000,00	3 738,32	2022	Esselmann Technika Pojazdowa Sp. z o.o. Sp. k.	Zgubienie świadectwa pracy pracownika i niezgłoszenie tego faktu do UODO
14	4 900 000,00	1 144 859,81	2022	Fortum Marketing and Sales Polska S.A.	Niewdrożenie odpowiednich środków technicznych i organizacyjnych przez podmiot przetwarzający oraz brak kontroli w tym zakresie przez Administratora nad Podmiotem

15	545 000,00	127 336,45	2021	Santander Bank Polska S. A.	Brak zawiadomienia osób których dane dotyczą o ryzyku dla i praw i wolności
16	18 000,00	4 205,61	2022	Pactum Poland Sp. z o.o.	Brak współpracy z organem nadzorczym polegający na niezapewnieniu dostępu do danych osobowych i innych informacji niezbędnych do realizacji jego zadań
17	45 000,00	10 514,02	2021	Politechnika Warszawska	Niezastosowanie odpowiednich środków technicznych i organizacyjnych mających zapewnić zdolność do ciągłego zapewnienia poufności usług przetwarzania, także za brak regularnego testowania, mierzenia i oceniania skuteczności środków
18	363 000,00	84 813,08	2021	Bank Millenium	Brak poinformowania UODO o naruszeniu oraz niewłaściwe poinformowanie osób których dane dotyczą
19	10 000,00	2 336,45	2021	Prezes Sądu Rejonowego w Zgierzu	Niewdrożenie adekwatnych środków technicznych - zgubienie niezaszyfrowanego Pendrive
20	160 000,00	37 383,18	2021	ERGO Hestia S.A.	Niezgłoszenie naruszenia oraz brak powiadomienia osoby której dane dotyczą
21	100 000,00	23 364,49	2021	P4	Brak zawiadomienia o naruszeniu ochrony danych
22	22 000,00	5 140,19	2021	Funeda Sp. z o.o.	Brak odpowiedzi na wezwania UODO - brak współpracy
23	22 000,00	5 140,19	2021	PNP S.A.	Brak odpowiedzi na wezwania UODO - brak współpracy
24	13 000,00	3 037,38	2021	Fundacja Promocji Mediacji i Edukacji Prawnej Lex	Brak zgłoszenia naruszenia do UODO oraz powiadomienia osób których dane dotyczą
25	1 100 000,00	257 009,35	2021	Cyfrowy Polsat	Niewdrożenie adekwatnych środków technicznych i organizacyjnych, które wymusiłyby na podmiocie przetwarzającym sprawne informowanie Administratora o naruszeniu danych

26	136 000,00	31 775,70	2021	ENEA S.A.	Przesłanie maila z danymi osoby do innego odbiorcy i niezgłoszenie naruszenia do UODO
27	21 000,00	4 906,54	2021	Anwara Sp. z o.o.	Brak współpracy z UODO
28	100 000,00	23 364,49	2021	Krajowa Szkoła Sądownictwa i Prokuratury	Niewdrożenie adekwatnych środków technicznych i organizacyjnych
29	85 000,00	19 859,81	2021	Placówka Medyczna	Niewykonanie decyzji administracyjnej w zakresie poinformowania osób, których dotyczyło naruszenie o naruszeniu ich danych
30	12 000,00	2 803,74	2021	Smart Cities	Brak współpracy z UODO
31	25 000,00	5 841,12	2021	Śląski Uniwerystet Medyczny	Brak powiadomienia osób których dotyczyło naruszenie
32	1 069 850,00	249 964,95	2020	ID Finance Poland	Niezdolność do szybkiego stwierdzenia zagrożenia i jego usunięcia
33	85 588,00	19 997,20	2020	Warta S.A.	Niezgłoszenie naruszenia po przesłaniu umowy do niewłaściwego odbiorcy
34	1 900 000,00	443 925,23	2020	Virgin Mobile Polska	Spółka nie przeprowadzała regularnych i kompleksowych testów, pomiarów i oceny skuteczności zastosowanych środków technicznych i organizacyjnych
35	50 000,00	11 682,24	2020	SGGW w Warszawie	Naruszenie - kradzież laptopa z danymi
36	100 000,00	23 364,49	2020	Główny Geodeta Kraju z siedzibą w Warszawie	Brak współpracy z UODO oraz niedostosowanie się do decyzji UODO
37	5 000,00	1 168,22	2020	Niepubliczny żłobek i przedszkole	Brak współpracy z UODO w związku z naruszeniem
38	15 000,00	3 504,67	2020	East Power sp. z o.o.	Brak współpracy z UODO

RODO to nie fikcja – zgłoszone skargi i naruszenia

- **2018**
  - Skargi: 5500
- **2019**
  - Skargi: 9314
  - Zgłoszone naruszenia: 6700
- **2020**
  - Skargi: 6442
  - Zgłoszone naruszenia: 7500
- **2021**
  - Skargi: 8300
  - Zgłoszone naruszenia: 13 000
- **2022**
  - Skargi: 7000
  - Zgłoszone naruszenia: 12 777

Fundusze Europejskie

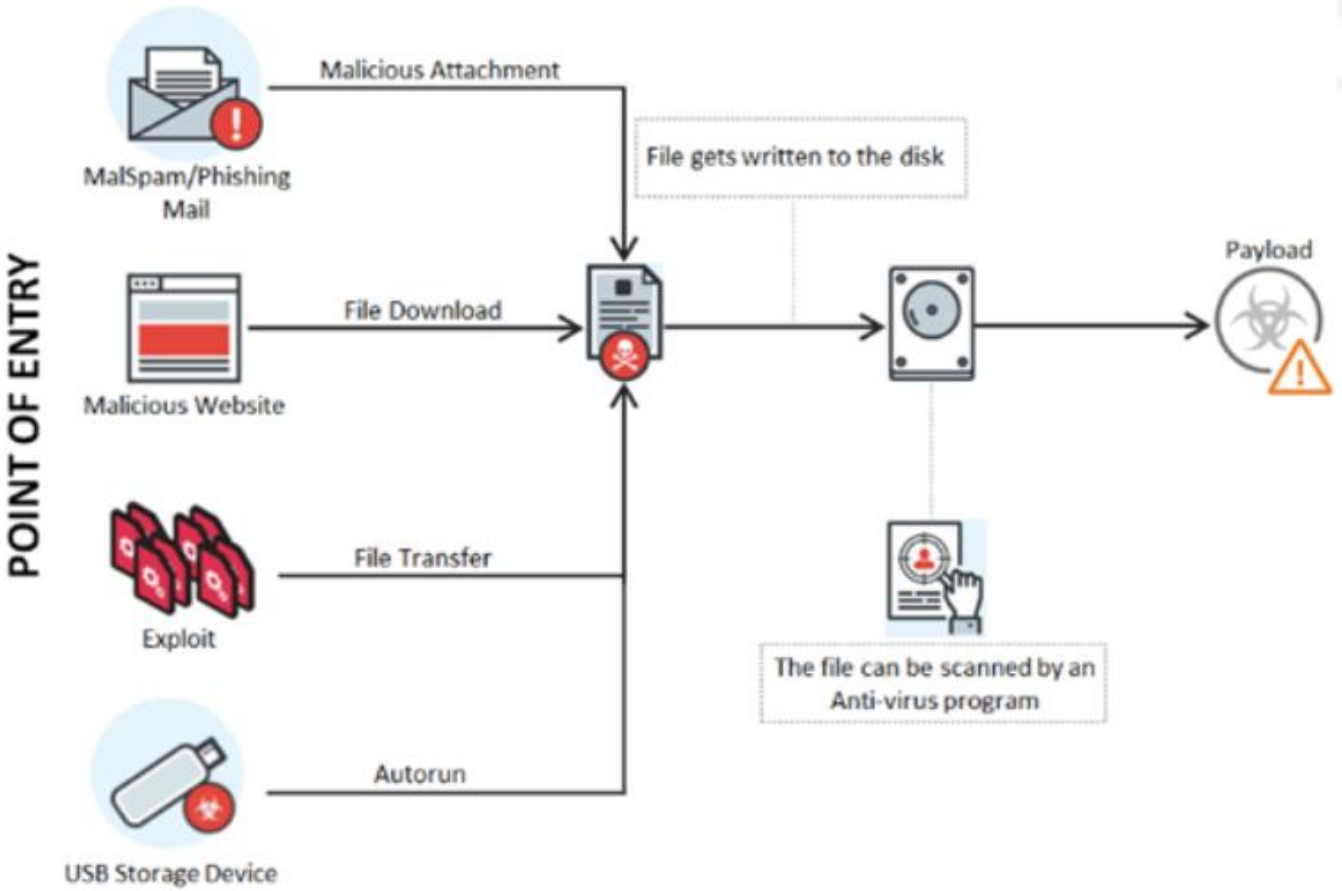
Konsekwencje niewłaściwego stosowania przepisów RODO w programie Fundusze Europejskie dla Łódzkiego 2021-2027 - co robić aby ich uniknąć – RODO a Cyberbezpieczeństwo dlaczego te obszary są nierozłączne

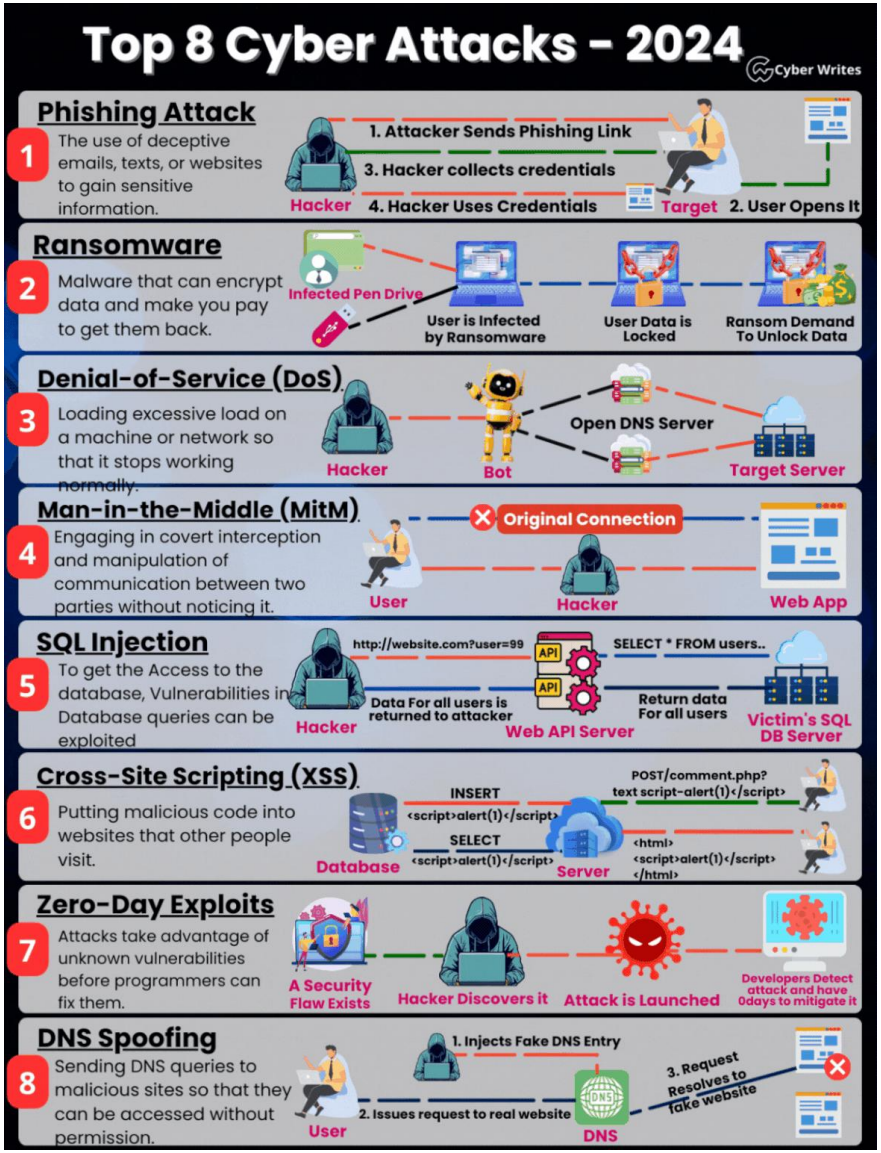
Fundusze Europejskie dla Łódzkiego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
ŁÓDZKIE

Wdrożone zabezpieczenia vs świadomość w zakresie bezpieczeństwa

Wdrożone zabezpieczenia vs świadomość w zakresie bezpieczeństwa

Wektory wejścia




Top 8 Cyber Attacks - 2024
Cyber Writes
Phishing Attack
1
The use of deceptive emails, texts, or websites to gain sensitive information.
1. Attacker Sends Phishing Link
3. Hacker collects credentials
Hacker
4. Hacker Uses Credentials
Target
2. User Opens It
Ransomware
2
Malware that can encrypt data and make you pay to get them back.
Infected Pen Drive
User is Infected by Ransomware
User Data is Locked
Ransom Demand To Unlock Data
Denial-of-Service (DoS)
3
Loading excessive load on a machine or network so that it stops working normally.
Hacker
Bot
Open DNS Server
Target Server
Man-in-the-Middle (MitM)
4
Engaging in covert interception and manipulation of communication between two parties without noticing it.
Original Connection
User
Hacker
Web App
SQL Injection
5
To get the Access to the database, Vulnerabilities in Database queries can be exploited
http://website.com?user=99
SELECT * FROM users..
API
API
Hacker
Data For all users is returned to attacker
Web API Server
Return data For all users
Victim's SQL DB Server
Cross-Site Scripting (XSS)
6
Putting malicious code into websites that other people visit.
INSERT
<script>alert(1)</script>
POST/comment.php?
text script-alert(1)</script>
SELECT
<script>alert(1)</script>
Database
Server
<html>
<script>alert(1)</script>
</html>
Zero-Day Exploits
7
Attacks take advantage of unknown vulnerabilities before programmers can fix them.
A Security Flaw Exists
Hacker Discovers it
Attack is Launched
Developers Detect attack and have 0days to mitigate it
DNS Spoofing
8
Sending DNS queries to malicious sites so that they can be accessed without permission.
1. Injects Fake DNS Entry
User
2. Issues request to real website
DNS
3. Request Resolves to fake website

Zagrożenia

❑ Pliki wykonywalne: programy, biblioteki, sterowniki:

- magic number „PE”: .exe, .acm, .ax, .cpl, .dll, .drv, .efi, .mui, .ocx, .scr, .sys
- instalki: .msi, .msp
- aplikacja Java: .jar

❑ Skrypty: bash, VBS, makra Office, JavaScript, Pyhton, Powershell:

- vbs, .js, .bat, .wsf, .hta, bash, .ps1

❑ Dokumenty:

- Office - URL wewnątrz, macro, exploity na Office’a, złośliwy plik wewnątrz dokumentu
- RTF - URL wewnątrz, złośliwy plik wewnątrz dokumentu
- PDF - linki do złośliwych stron, złośliwy plik wewnątrz dokumentu, automatyczne uruchomienie obiektów JavaScript w pdfie, exploity na Adobe Readera

Zagrożenia

❑ Inne:

- zdjęcia, wideo - exploity na programy uruchamiające pliki,
- pliki skróty - link do uruchomienia programu z zakodowanym argumentem do pobrania i uruchomienia malware'u.

Pliki mogą zawierać „exploita" albo wykorzystywać legitne funkcje programu uruchamiającego.

Zagrożenia!!!

Phishing

- Wyłudzanie informacji to mechanizm tworzenia wiadomości, które wykorzystują techniki inżynierii społecznej (socjotechniki), aby odbiorca został zwabiony i „wziął przynętę”.
- Phisherzy próbują zwabić odbiorców, aby:
  - **otworzyć złośliwy załącznik**, np. „włącz zawartość” - makro uruchamia skrypt (.js, ps1),
  - **kliknąć niebezpieczny adres URL,**
  - **przekazać swoje dane uwierzytelniające** za pośrednictwem dobrze wyglądających stron phishingowych .
- Phishing wykorzystywany w ponad 90% przypadków do infekcji złośliwvm oprogramowaniem i 72% naruszeń danych w organizacjach.

- skok w pierwszym miesiącu pandemii o **667%** phishingu.

Zagrożenia!!!

- **Spoofing** - to rodzaj ataku, w którym przestępcy podszywają się pod banki, instytucje i urzędy państwowe, firmy, a nawet osoby fizyczne w celu wyłudzenia od swoich ofiar danych lub pieniędzy.
- **Smishing** - to rodzaj phishingu skierowanego na telefony komórkowe. Celem przestępcy jest zgromadzenie danych osobowych, takich jak na przykład numer ubezpieczenia społecznego lub numer karty kredytowej. Drogą ataku są wiadomości tekstowe lub SMS.
- **Vishing** jest to wyłudzanie danych w trakcie rozmowy telefonicznej. Zręczni rozmówcy podający się za bankowców, doradców inwestycyjnych czy instytucje zaufania publicznego, są w stanie tak zmanipulować rozmówcę, że ten ujawni swoie szczegółowe dane.
- **Qrishing**

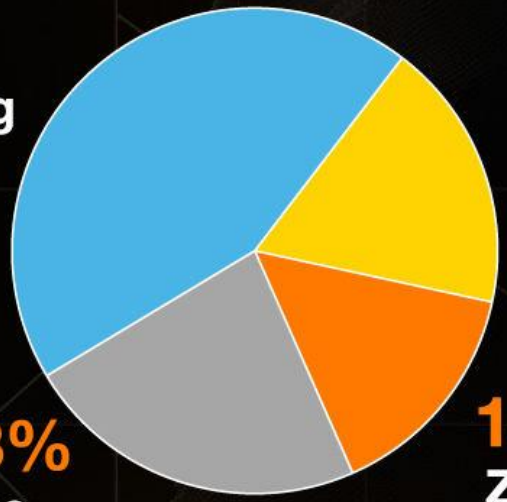
Zagrożenia!!!

❑ **Raport Orange CERT Polska dot. bezpieczeństwa**

- Systemy bezpieczeństwa operatora zablokowały w zeszłym roku **ponad 360 tysięcy fałszywych stron internetowych**. To rekordowa **liczba, trzykrotnie większa niż rok wcześniej**

- W linki prowadzące do stron **stworzonych przez oszustów** kliknęło około **5,5 mln internautów**

TOP 3 zagrożeń 2023 wg CERT Orange Polska



44%
Phishing

18%
Ataki DDoS

15%
Złośliwe oprogramowan

23%
Inne

CERT Orange Polska

Raport CERT Orange Polska za rok 202

Phishing: w jakie linki najczęściej klikali internauci

52%
Fałszywe inwestycje

18%
Płatności, w tym oszustwo na kupującego

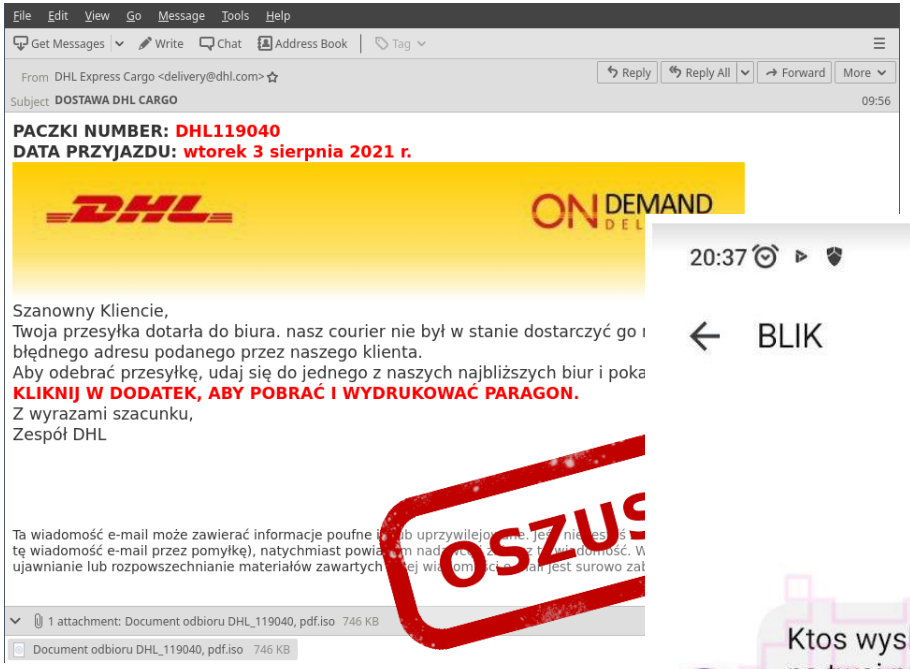
7%
Fałszywe sklepy

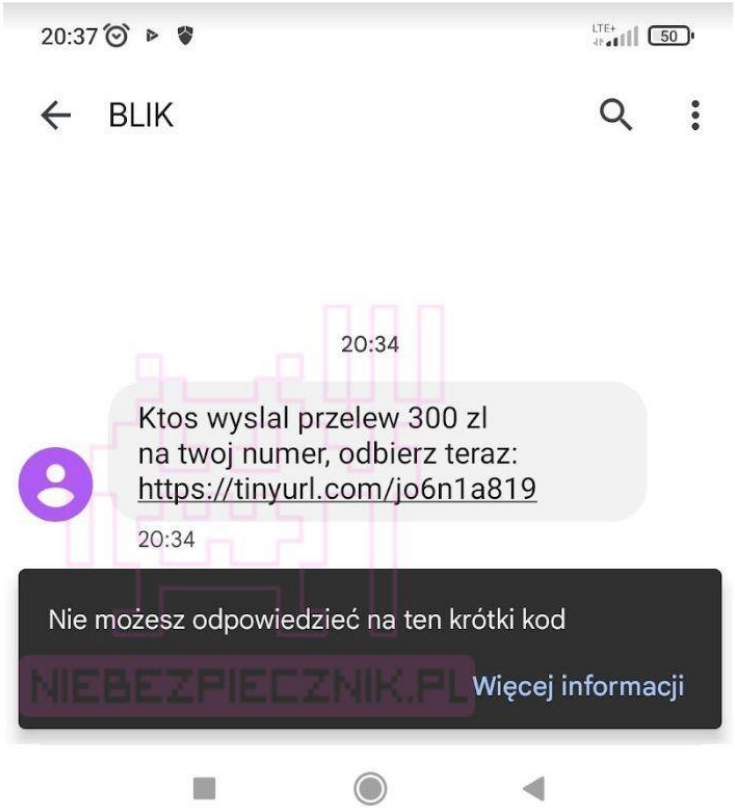
CERT Orange Polska

Raport CERT Orange Polska za rok 2023

Zagrożenia!!!

- Phishing, spoofing, vishing, smishing





Zagrożenia!!!

Czy mogliby Państwo natychmiast zapoznać się z załączoną specyfikacją zamówienia, a następnie przesłać nam fakturę proforma.

Oczekiwanie na szybką reakcję.

Z wyrazami szacunku
Daria Jasińska
Dyrektor Zarządzający
SPECYFIKACJA ZAMÓWIENIA PDF.PNG

Zagrożenia!!!

Czy mogliby Państwo natychmiast zapoznać się z załączoną specyfikacją zamówienia, a następnie przesłać nam fakturę proforma.

Oczekiwanie na szybką reakcję.

Z wyrazami szacunku
Daria Jasińska
Dyrektor Zarządzający
SPECYFIKACJA ZAMÓWIENIA PDF.PNG

Zagrożenia!!!

Od Monika Janecka <info@gevex.hu>

Do undisclosed-recipients:;

Temat **Zapłata**

Odpowiedz

Dzień dobry,

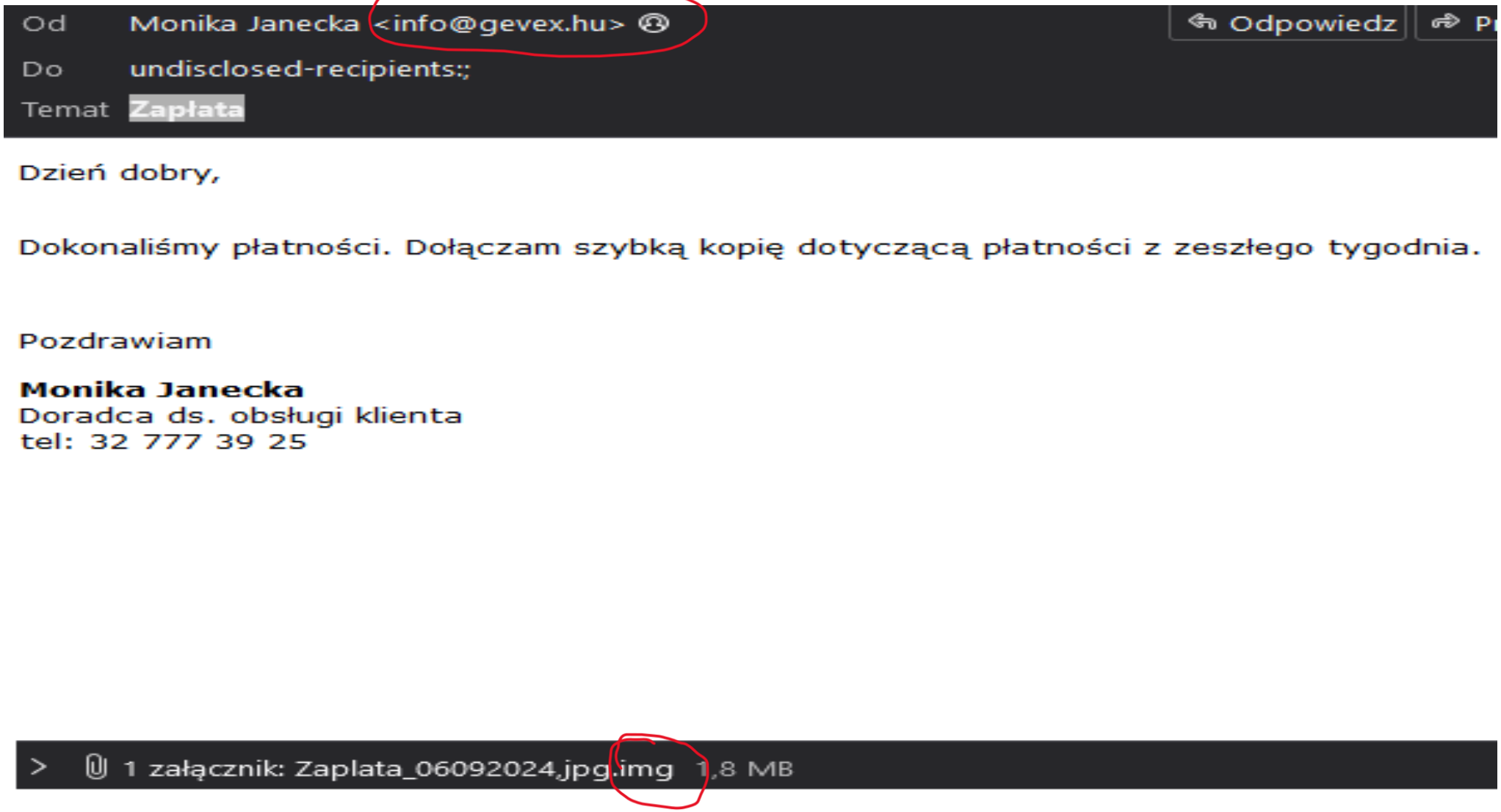
Dokonaliśmy płatności. Dołączam szybką kopię dotyczącą płatności z zeszłego tygodnia.

Pozdrawiam

Monika Janecka
Doradca ds. obsługi klienta
tel: 32 777 39 25

> 1 załącznik: Zaplata_06092024.jpg.img 1,8 MB

Zagrożenia!!!



Od Monika Janecka <info@gevex.hu>

Odpowiedz

Do undisclosed-recipients:;

Temat Zapłata

Dzień dobry,

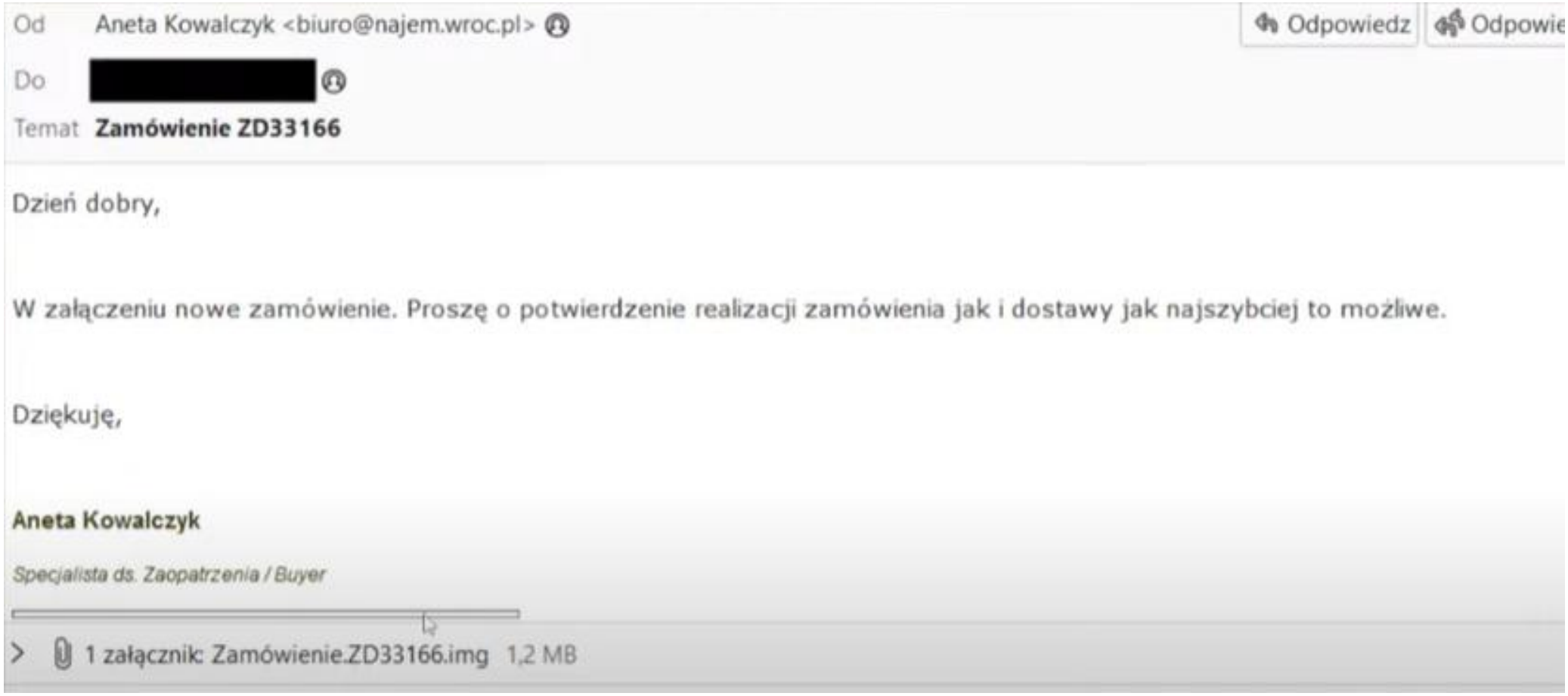
Dokonaliśmy płatności. Dołączam szybką kopię dotyczącą płatności z zeszłego tygodnia.

Pozdrawiam

Monika Janecka
Doradca ds. obsługi klienta
tel: 32 777 39 25

1 załącznik: Zaplata_06092024.jpg.img 1,8 MB

Zagrożenia!!!



Od Aneta Kowalczyk <biuro@najem.wroc.pl>

Odpowiedz Odpowie

Do [redacted]

Temat **Zamówienie ZD33166**

Dzień dobry,

W załączeniu nowe zamówienie. Proszę o potwierdzenie realizacji zamówienia jak i dostawy jak najszybciej to możliwe.

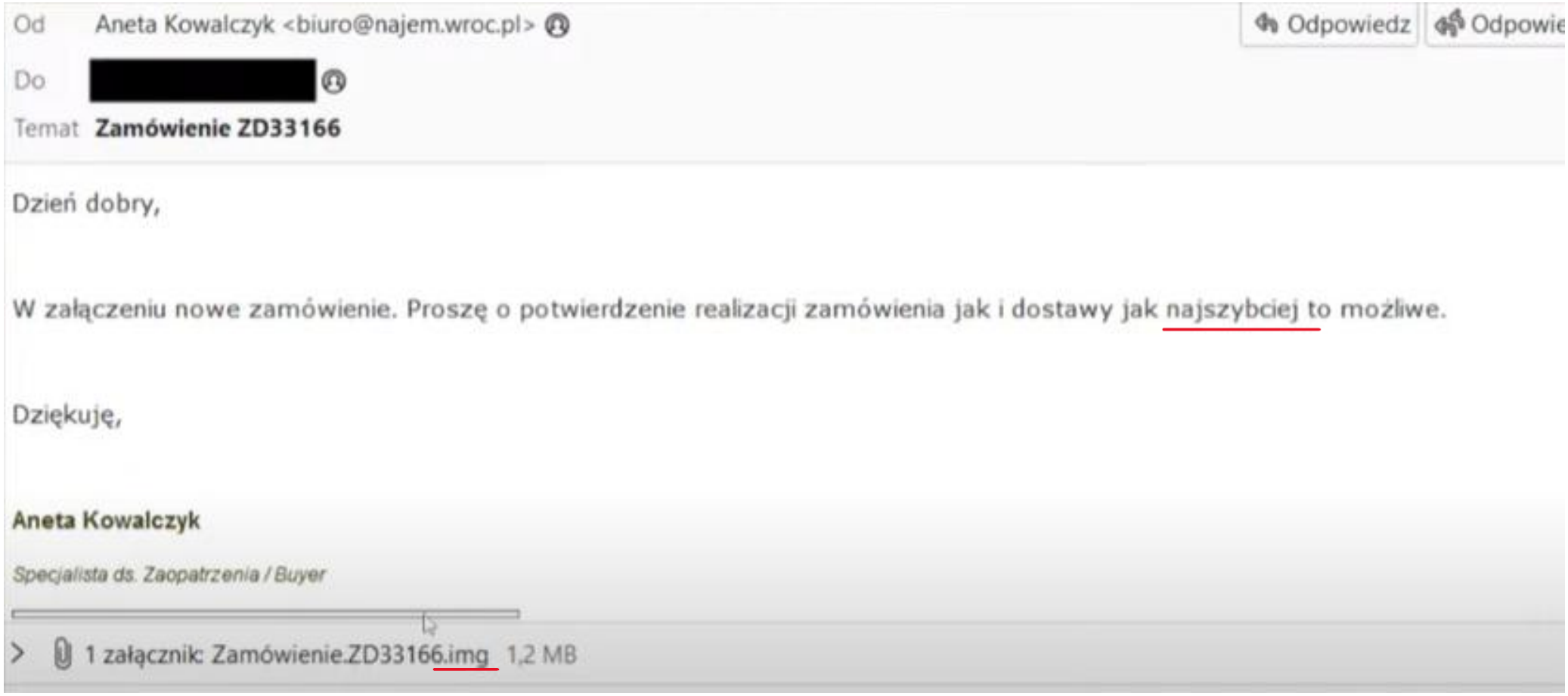
Dziękuję,

Aneta Kowalczyk

Specjalista ds. Zaopatrzenia / Buyer

1 załącznik: Zamówienie.ZD33166.img 1,2 MB

Zagrożenia!!!



Od Aneta Kowalczyk <biuro@najem.wroc.pl>

Odpowiedz Odpowie

Do [redacted]

Temat **Zamówienie ZD33166**

Dzień dobry,

W załączeniu nowe zamówienie. Proszę o potwierdzenie realizacji zamówienia jak i dostawy jak najszybciej to możliwe.

Dziękuję,

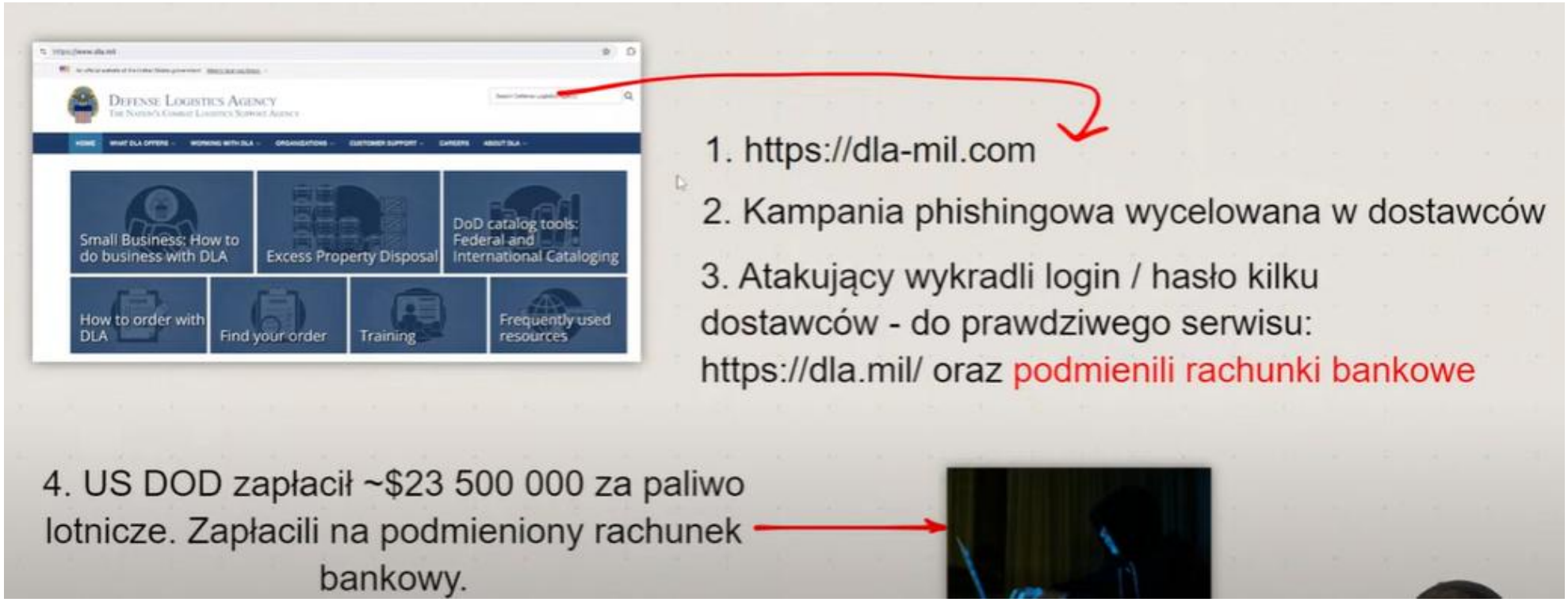
Aneta Kowalczyk

Specjalista ds. Zaopatrzenia / Buyer

1 załącznik: Zamówienie.ZD33166.img 1,2 MB

Zagrożenia!!!

- **Phishing, spoofing, vishing, smishing**



Zagrożenia!!!

- **Brak weryfikacji osoby**

MGM wyłącza automaty do gier / bankomaty w kasynach w Las Vegas

"wejście na Linkedin, znalezienie pracownika, a następnie telefon do działu pomocy technicznej. Firma wyceniana na 33 900 000 000 dolarów została pokonana w 10-minutowej rozmowie".

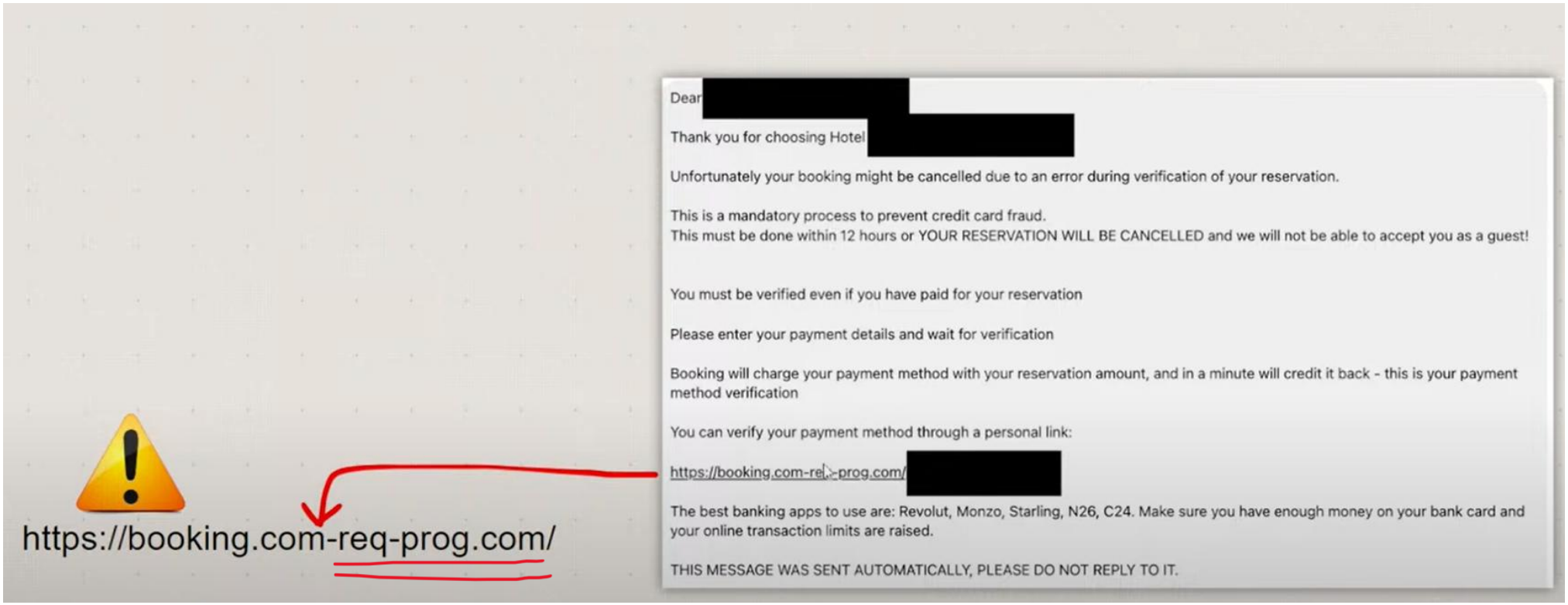
Zagrożenia!!!

- Czy poniższy adres strony jest adresem strony booking com?

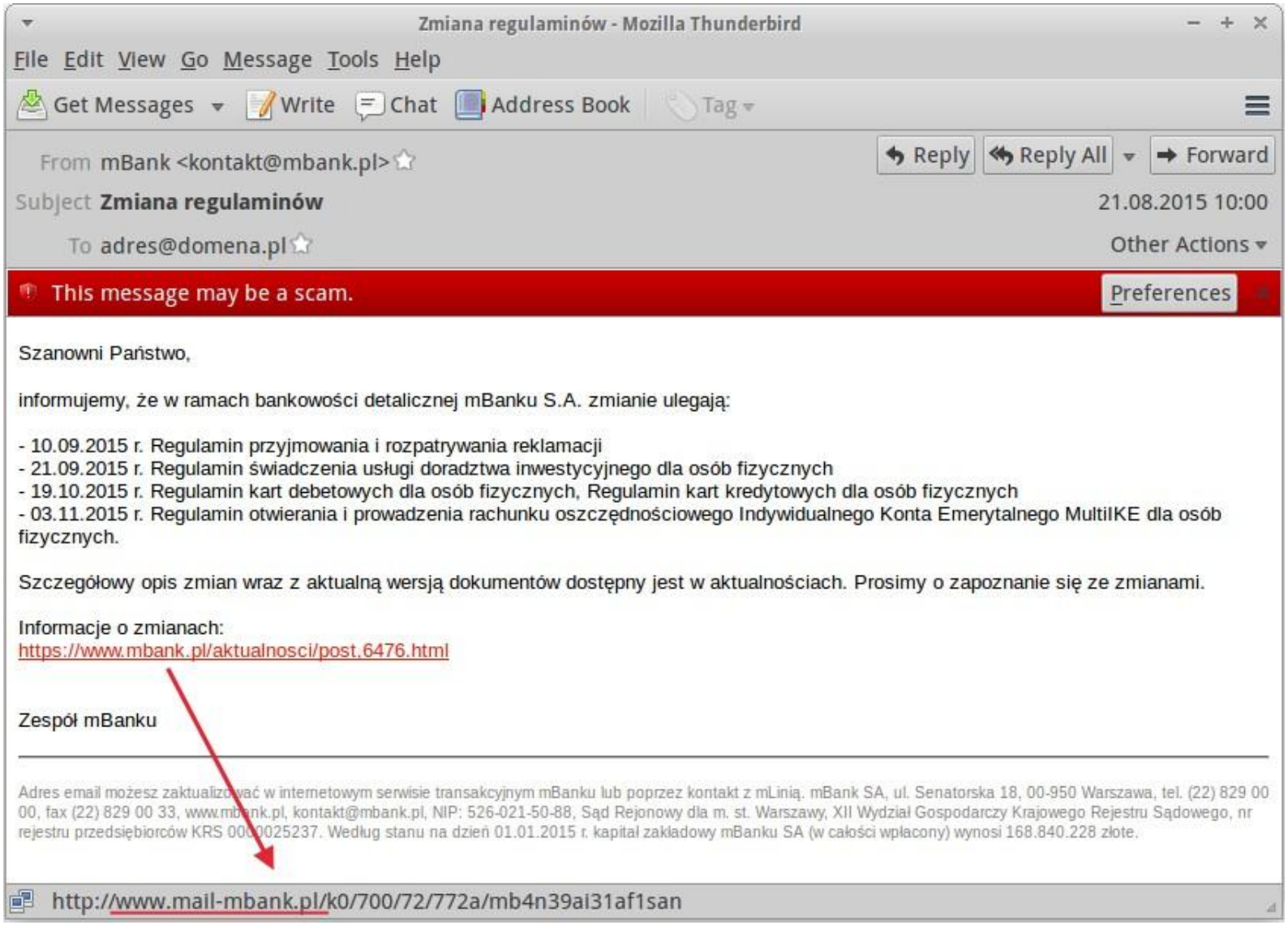
https://booking.com-reg-prog.com/

Zagrożenia!!!

- **Phishing, spoofing, vishing, smishing**

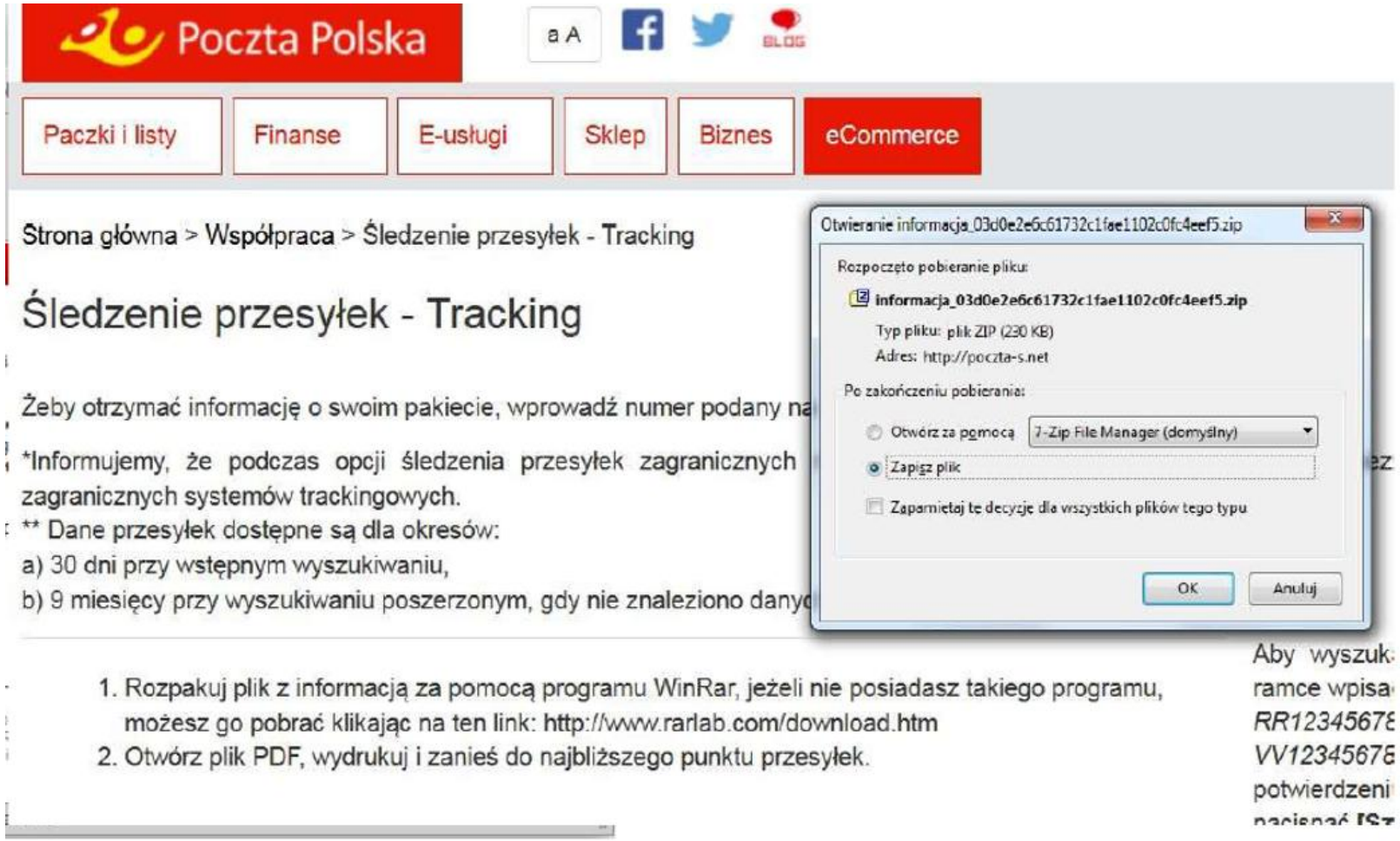


Zagrożenia!!!

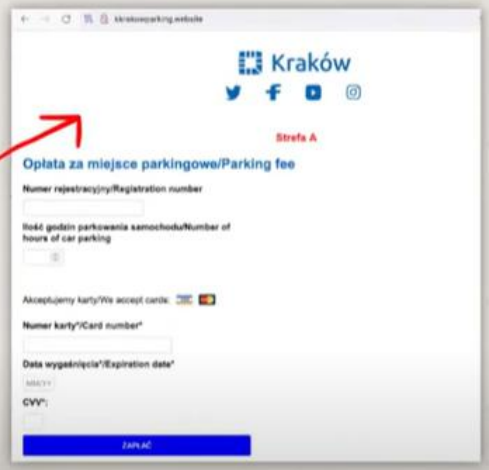

Zmiana regulaminów - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages
Write
Chat
Address Book
Tag
From mBank <kontakt@mbank.pl>
Reply
Reply All
Forward
Subject Zmiana regulaminów
21.08.2015 10:00
To adres@domena.pl
Other Actions
This message may be a scam.
Preferences
Szanowni Państwo,
informujemy, że w ramach bankowości detalicznej mBanku S.A. zmianie ulegają:
- 10.09.2015 r. Regulamin przyjmowania i rozpatrywania reklamacji
- 21.09.2015 r. Regulamin świadczenia usługi doradztwa inwestycyjnego dla osób fizycznych
- 19.10.2015 r. Regulamin kart debetowych dla osób fizycznych, Regulamin kart kredytowych dla osób fizycznych
- 03.11.2015 r. Regulamin otwierania i prowadzenia rachunku oszczędnościowego Indywidualnego Konta Emerytalnego MultiIKE dla osób fizycznych.
Szczegółowy opis zmian wraz z aktualną wersją dokumentów dostępny jest w aktualnościach. Prosimy o zapoznanie się ze zmianami.
Informacje o zmianach:
https://www.mbank.pl/aktualnosci/post,6476.html
Zespół mBanku
Adres email możesz zaktualizować w internetowym serwisie transakcyjnym mBanku lub poprzez kontakt z mLinią. mBank SA, ul. Senatorska 18, 00-950 Warszawa, tel. (22) 829 00 00, fax (22) 829 00 33, www.mbank.pl, kontakt@mbank.pl, NIP: 526-021-50-88, Sąd Rejonowy dla m. st. Warszawy, XII Wydział Gospodarczy Krajowego Rejestru Sądowego, nr rejestru przedsiębiorców KRS 0000025237. Według stanu na dzień 01.01.2015 r. kapitał zakładowy mBanku SA (w całości wpłacony) wynosi 168.840.228 złote.
http://www.mail-mbank.pl/k0/700/72/772a/mb4n39ai31af1san

Zagrożenia!!!

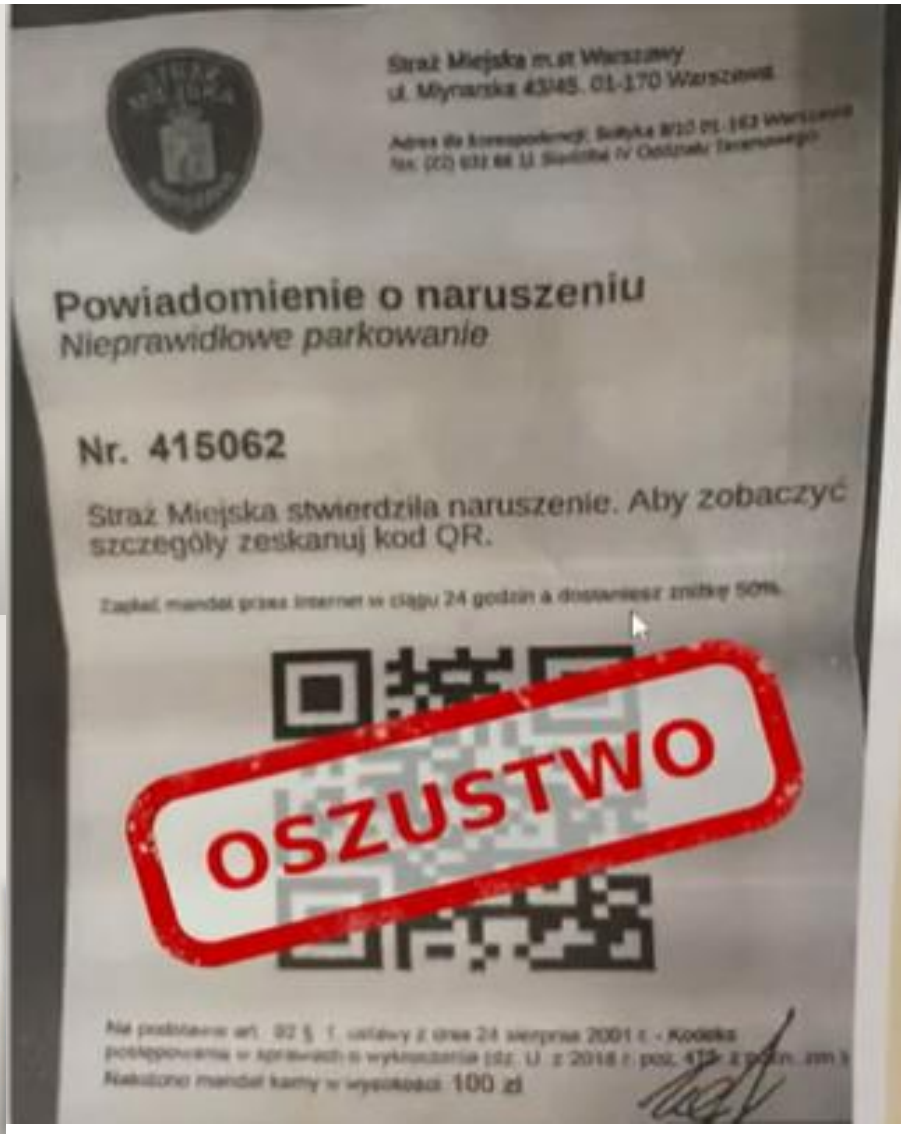
- **Phishing, spoofing, vishing, smishing**



Fałszywe kody QR na parkingach w Krakowie

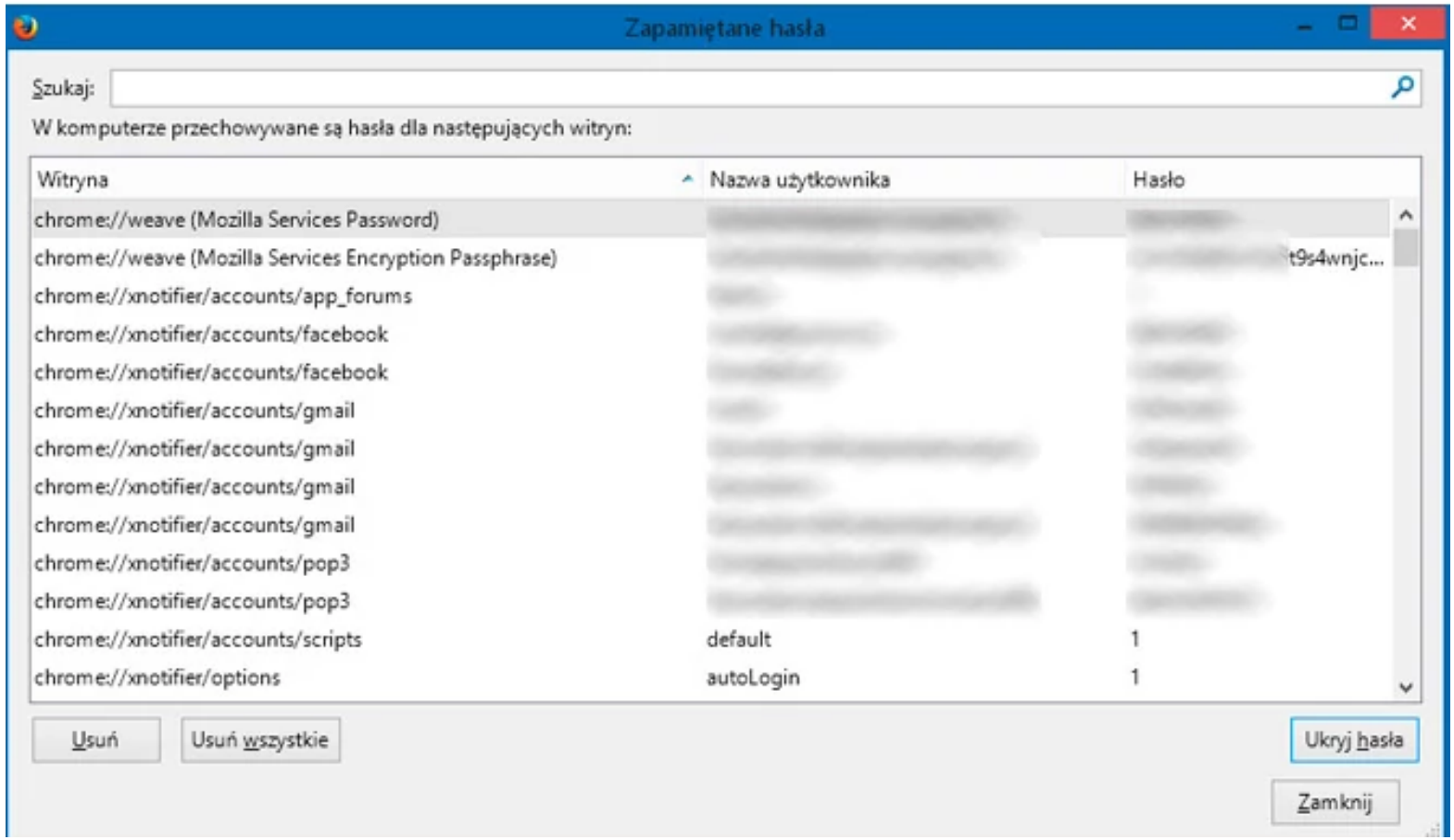


- QR kod to nośnik danych (często zawiera po prostu link)
  Link może być złośliwy bądź normalny
- QR kod naklejony fizycznie, wyglądający profesjonalnie,
  wcale nie musi oznaczać "normalności" linku
- Uwaga na skanowanie kodów QR w aplikacji Wiadomości
  (Android)



Zagrożenia!!!

- Zapamiętane hasła w przeglądarkach



Zagrożenia!!!

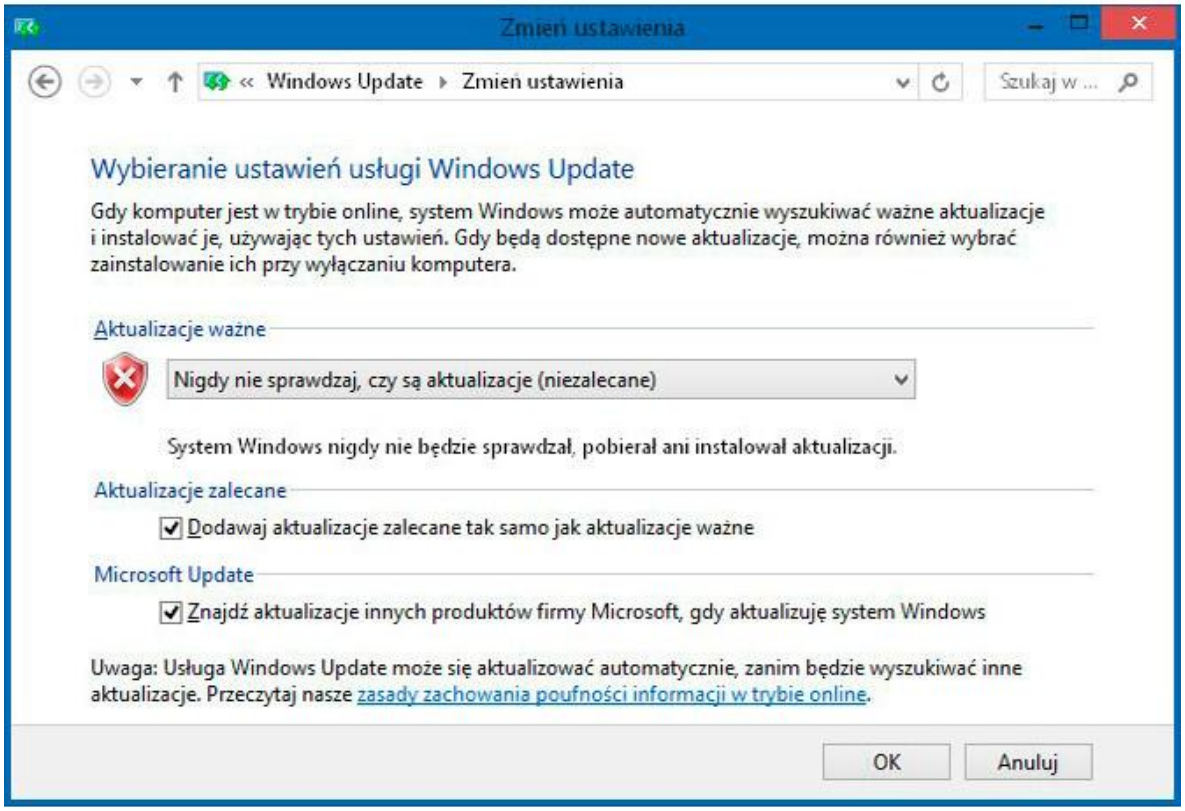
- **Malware – Ransomware**
- **Słabe hasła,**
- **Phishing,**
- **Niezaufane urządzenia,**

Zagrożenia!!!

- **Otwarte sieci Wi-Fi**

Zagrożenia!!!

- **Nieaktualizowane oprogramowanie**



Podstawowe zasady bezpieczeństwa

- ❑ **Stosuj:**
- **odpowiednio złożone i długie hasła – idealnie 4+ nieoczywiste sklejone słowa >= 15 znaków, np. smiesznelatwedozapamietania,**
- **nie stosuj tych samych haseł do różnych systemów,**
- ❑ **używaj menadżerów haseł: Bitwarden, KeePass,**
- ❑ **Stosuj dwuskładnikowe uwierztelnianie: klucze 2FA (yubico.com) , authenticator, passkey,**
- ❑ **Bądź czujny – czytaj komunikaty, w razie najmniejszych wątpliwości zwracaj się do ASI,**
- ❑ **Regularny backup - ODSEPAROWANY OD ŚRODOWISKA PROGUKCYJNEGO – 3x2x1,**
- ❑ **Instaluj aktualizacje,**
- ❑ **Stosuj wyłącznie legalne oprogramowanie,**
- ❑ **Sprawdzaj adres nadawcy maila a nie jego nazwę,**
- ❑ **Nie otwieraj załączników od nieznanych nadawców lub też takich, których nie rozpoznajesz nawet jak pochodzą o Twoich znajomych.**

Podstawowe zasady bezpieczeństwa

- ❑ Nie klikaj w linki w wiadomościach mailowych – sprawdzaj do jakiej lokalizacji faktycznie odsyła link.
- ❑ Nie skanuj kodów QR z miejsc niesprawdzonych.
- ❑ Nie klikaj w linki w SMS-ach.
- ❑ Uważaj na fałszywe oferty, np. fałszywe rekrutacje oraz deepfake (5s) (elevenlabs.io).
- ❑ Uważaj na fleepery/proxmarki.
- ❑ Stosuj Ad – blocker, np. uBlock Origin – pamiętaj że reklama może odsyłać do fałszywej strony.

Podstawowe zasady bezpieczeństwa

- **Nie podłączaj niezaufanych urządzeń przenośnych do komputera, ani też swoich urządzeń do niezaufanych miejsc.**

TIME IT TAKES FOR A HACKER TO CRACK YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

HIVE SYSTEMS

Cybersecurity that's approachable.

Find out more at hivesystems.io

Podstawowe zasady bezpieczeństwa

- Pamiętaj, że maile od klienta/kontrahenta/pracodawcy/kolegi/koleżanki mogą zawierać złośliwe linki / załączniki (skrzynka osoby mogła zostać zhackowana)
- Pamiętaj, że na „zaufanej” domenie (adresie) również mogą znajdować się fałszywe formularze logowania (domena mogła zostać zhackowana)
- Pamiętaj, że antywirusy, inne systemy wykrywające złośliwe oprogramowanie / linki, mogą okazać się zawodne
- Pamiętaj, że 2FA bazujące np. na kodach generowanych przez appkę, może zostać oszukane (jeśli podasz kod na podstawionej stronie)
- Najlepszym „firewallem” jest głowa / edukacja /świadomość zagrożeń

Zagrożenia!!!

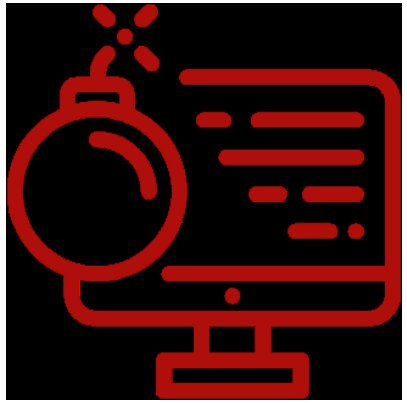
- **Naiwność - przekonanie, że mnie to nie dotyczy.**

Obsługa naruszeń przy przetwarzaniu danych

Naruszenie czy incydent? – art. 33

- Naruszenie czy incydent?
- Przez pojęcie „naruszenia ochrony danych osobowych” należy rozumieć **„naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych”** (art. 4 pkt 12 RODO)

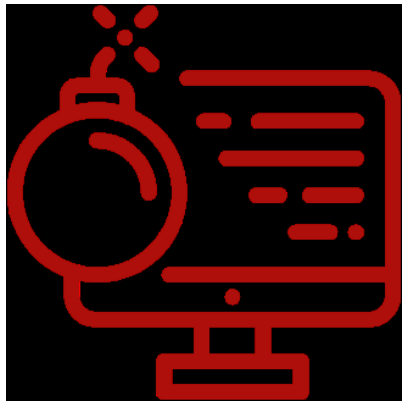
- Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.



Naruszenie czy incydent? – art. 33

NARUSZENIE POUFNOŚCI

- Przypadkowe wysłanie danych osobowych klienta do niewłaściwego działu firmy lub osoby postronnej
- System informatyczny administratora został zainfekowany złośliwym oprogramowaniem. Po przeprowadzeniu wstępnej analizy administrator stwierdził, że w wyniku działania tego oprogramowania osoba nieupoważniona uzyskała dostęp do danych osobowych.



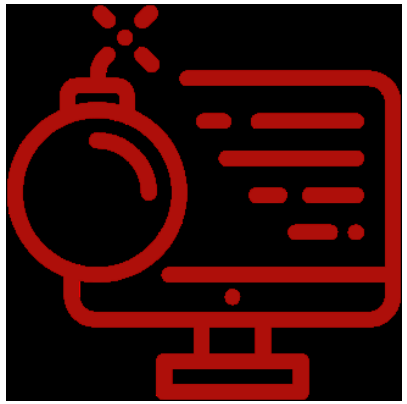
Naruszenie czy incydent? – art. 33

NARUSZENIE DOSTĘPNOŚCI

- Zgubienie lub kradzież nośnika zawierającego bazy danych klientów administratora przy braku kopii zapasowej.
- Pracownik przypadkowo lub osoba nieupoważniona celowo usuwa dane ze zbioru. Administrator próbuje odzyskać dane z kopii zapasowej, jednak jego działania nie przynoszą rezultatu.
- W wyniku przerwy w dostawie prądu lub ataku typu „odmowa usługi” (tzw. DDoS), administrator tymczasowo lub trwale traci dostęp do danych osobowych.

NARUSZENIE INTEGRALNOŚCI

- Pracownik dla żartu zmienia nazwiska klientów poprzez dopisanie litery „s” na końcu każdego z nich.



Obowiązki w zakresie zgłaszania naruszeń

- W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
- Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi. **Informacja o naruszeniu powinna:**
  - opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,

Obowiązki w zakresie zgłaszania naruszeń

- zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
- opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
- opisywać środki zastosowane lub proponowane przez podmiot w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków,
- dodatkowe informacje umożliwiające Instytucji Pośredniczącej oraz Instytucji Zarządzającej określenie, czy naruszenie skutkuje wysokim ryzykiem naruszenia praw lub wolności osób fizycznych.

Omówienie formularza zgłoszenia naruszenia do UODO

Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych – art. 34 - przykład

- Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
- Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach :
  - administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,
  - administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
  - wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek.

Dobre praktyki przy przetwarzaniu danych osobowych

Dobre praktyki w ochronie danych osobowych

- Za bezpieczeństwo przetwarzania danych osobowych w określonym procesie przetwarzania indywidualną odpowiedzialność ponosi każdy pracownik mający dostęp i upoważnienie do danych osobowych.
- Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem związanym z zakresem obowiązków służbowych w ramach udzielonego upoważnienia do przetwarzania danych.
- Pracownicy przechowujący dane osobowe zobowiązani są do zabezpieczenia materiałów zawierających dane w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym. Dane osobowe w formie papierowej muszą być przechowywane w szafach zamykanych na klucz. Klucze należy przechowywać w sposób bezpieczny bez możliwości dostępu do nich osób nieuprawnionych – **zawsze przy opuszczaniu stanowiska pracy (nawet na chwilę) pamiętaj o zabezpieczeniu dokumentów oraz komputera**

Dobre praktyki w ochronie danych osobowych

- Zawsze istnieje ryzyko, że osoby niepowołane/trzecie mogą podsłuchać rozmowę w której podawane są dane osobowe, dlatego zawsze **bądź ostrożny i świadomy otoczenia, gdy omawiasz sprawy poufne.**
- Nie wolno **przekazywać danych w żadnej formie** (elektronicznej, papierowej) **osobom trzecim**, które nie są uprawnione do dostępu do nich.
- Ze względu na fakt, iż nigdy nie mamy pewności co do tożsamości osoby, z którą rozmawiamy przez telefon, **nie wolno udzielać informacji, w których podawane są dane osobowe w formie zapytania telefonicznego bez uprzedniej identyfikacji osoby.**
- Wszystkie zbędne dane w formie kopii powstałe w procesie przetwarzania muszą zostać niezwłocznie zniszczone w sposób uniemożliwiający ich odczytanie.

Dobre praktyki w ochronie danych osobowych

- Przy przetwarzaniu danych osobowych podczas kontaktu z klientami na biurku mogą znajdować się dokumenty z danymi osobowymi tylko osoby, z którą w danym momencie załatwiamy formalności. **Nie wolno pozostawiać bez kontroli dokumentów z danymi osobowymi. Zawsze przy opuszczaniu stanowiska pracy (nawet na chwilę) dokumenty należy schować do szafki i zamknąć na klucz (zabrać klucz), uniemożliwiając w ten sposób dostęp do danych osobom trzecim, komputer należy zablokować (klawisze windows + L).**

- Pracownicy zobowiązani są do zamykania na klucz wszelkich pomieszczeń, w których przetwarzane są dane osobowe w czasie ich chwilowej nieobecności w pomieszczeniu w godzinach pracy jak i po jej zakończeniu, klucze nie mogą być pozostawione w zamku.

- Przebywanie osób nieuprawnionych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych, chyba że dane te są w odpowiedni sposób zabezpieczone przed dostępem.

Dobre praktyki w ochronie danych osobowych

- Ujawnianie przez użytkownika osobie trzeciej haseł tymczasowych, haseł osobistych lub innych haseł mu powierzonych jest zabronione.
- Zabrania się wynoszenia dokumentów zarówno w formie papierowej jak i elektronicznej zawierających dane osobowe poza biuro lub, jeśli to konieczne, należy uzyskać na to zgodę przełożonego.
- Opuszczając stanowisko pracy należy uporządkować biurko i zamknąć w szafach na klucz poufne dokumenty (zabrać klucz), sprawdzić czy w portach USB lub napędzie DVD nie pozostały nośniki z danymi.
- Nie wolno prosić osoby, której dane dotyczą o podanie danych osobowych, które wykraczają poza zakres niezbędny do wykonania zamierzonego celu.
- Zabrania się wykorzystywania danych osobowych w celach innych niż te, do których zostały zebrane i na które osoba zainteresowana wyraziła zgodę.
- Osobę, której dane dotyczą, należy informować o jej prawach i obowiązkach w sposób jasny i zrozumiały, dotyczy to również kwestii zgód.

Korzystanie ze służbowej poczty email

- Zabrania się przesyłania przez Pracownika dokumentów firmowych na swoje prywatne adresy e-mail.
- **Niezaszyfrowana poczta e-mail może służyć wyłącznie do przesyłania dokumentów, które nie zawierają danych osobowych, danych wrażliwych czy poufnych.**
- Nie wolno przesyłać niezaszyfrowaną pocztą e-mail **żadnych** danych osobowych Klientów oraz Pracowników, informacji o wysokości wynagrodzenia itp.
- Nie wolno prosić o przesłanie danych osobowych lub innych danych wrażliwych e-mailem, należy poprosić ewentualnie o dostarczenie danych bez określenia sposobu – jeżeli osoba, której dane dotyczą wyśle je e-mailem to robi to na własną odpowiedzialność (my ją o to nie prosiliśmy).

Korzystanie ze służbowego komputera

- Nigdy nie należy otwierać załączników ani klikać na linki w poczcie e-mail od nieznanych nadawców lub w wiadomościach, których się nie spodziewamy.
- Obowiązkiem Pracownika jest korzystanie ze służbowego komputera oraz oprogramowania wyłącznie w celach wykonywania obowiązków pracowniczych.
- Nie wolno podłączać do portów USB lub wkładać do napędów DVD nośników zewnętrznych prywatnych lub pochodzących z nieznanego źródła, nośniki te mogą zawierać wirusy komputerowe, które mogą stwarzać zagrożenie dla bezpieczeństwa komputera, sieci firmowej, a co się z tym wiąże, również danych osobowych przetwarzanych w firmie. W przypadku zaistnienia konieczności podłączenia w/w urządzenia należy skontaktować się z Administratorem Sieci Komputerowej w celu uprzedniego przeskanowania sprzętu pod kątem obecności złośliwego oprogramowania.
- Podczas użytkowania komputera zabrania się wchodzenia na strony internetowe, które mogą stwarzać zagrożenie dla systemu informatycznego i bezpieczeństwa danych. **Nie surfuj po internetowych stronach o niewłaściwej treści, nie ściągaj stamtąd żadnych plików.**
- Monitor komputera należy usytuować w taki sposób, aby osoby nieupoważnione wchodzące do pomieszczenia nie miały wglądu do danych na nim wyświetlanych.

Fundusze Europejskie

Dziękuję za uwagę

Robert Wakoń

tel. +48 609 181 180

e-mail: r.wakon@rProtection.com.pl

Fundusze Europejskie dla Łódzkiego

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

ŁÓDZKIE