Wyniki oceny skutków dla ochrony danych (DPIA) oraz analizy ryzyka

PrzykładowaOrganizacja sp. z o.o.

Warszawa, 15.12.2021 r.

METRYKA DOKUMENTU

Wersja:	DPIA sygnaliści	**Opis:**	
Data sporządzenia:	2021-12-15		

Sporządził:	Katarzyna Szczypińska	**Podpis:**	

SPIS TREŚCI

METRYKA DOKUMENTU 2
PODSUMOWANIE DLA NAJWYŻSZEGO KIEROWNICTWA 4
DEFINICJE 5
USTALENIA METODOLOGICZNE: CELE, ZAKRES, KRYTERIA, PODSTAWA AUDYTU 9
CEL 9
KRYTERIA 9
ZAKRES 9
OPIS METODYKI 9
USTALENIA KONTEKSTU PRZETWARZANIA 11
KONTEKST WEWNĘTRZNY ORAZ ZEWNĘTRZNY 11
ANALIZA RYZYKA DLA PROCESÓW (DPIA) 13
PROCES PRZETWARZANIA DANYCH W RAMACH SYSTEMU ZGŁASZANIA NARUSZEŃ PRZEZ SYGNALISTÓW 13
PLAN POSTĘPOWANIA Z RYZYKIEM PROCESÓW (DPIA) 19
MAPA ZALEŻNOŚCI I POWIĄZAŃ 20
ANALIZA RYZYKA DLA ZASOBÓW 21
PLAN POSTĘPOWANIA Z RYZYKIEM ZASOBÓW 22
MOŻLIWE KONSEKWENCJE STWIERDZONYCH NIEZGODNOŚCI 23
ZASADY MONITOROWANIA I PRZEGLĄDU 23

PODSUMOWANIE DLA NAJWYŻSZEGO KIEROWNICTWA

Celem przeprowadzenia niniejszego procesu było opisanie realizowanych przez organizację procesów przetwarzania danych osobowych oraz ocenienie ich konieczności i proporcjonalności, a także wspomożenie zarządzania ryzykiem naruszenia praw i wolności osób fizycznych wynikającym z przetwarzania danych osobowych poprzez ocenę ryzyka i określenie środków pozwalającym zaradzić tym czynnikom ryzyka.

Na podstawie przeprowadzanych działań zdefiniowano następujące procesy przetwarzania danych osobowych realizowane przez organizację:

1. Proces przetwarzania danych w ramach systemu zgłaszania naruszeń przez sygnalistów

Spośród wskazanych procesów obowiązek przeprowadzenia oceny skutków dla ochrony danych ustalono w stosunku do następujących procesów:

1. Proces przetwarzania danych w ramach systemu zgłaszania naruszeń przez sygnalistów

Powyższe oznacza, zgodnie z art. 35 ust. 1 RODO, że wskazane operacje przetwarzania ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, przez co administrator przed rozpoczęciem przetwarzania winien dokonać oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.

DEFINICJE

Użyte w niniejszym raporcie określenia należy rozumieć w następujący sposób:

1. **Administrator danych (Administrator)** - osoba fizyczna lub prawna, organ publiczny, jednostka 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 prawiepaństwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania (art. 4 pkt 7 RODO);
2. **Przedstawiciel ds. IT** - osoba wyznaczona przez administratora danych, która odpowiada za zapewnienie sprawności, należytej konserwacji i wdrażania technicznych zabezpieczeń systemów informatycznych oraz odpowiada za to, aby systemy informatyczne, w których przetwarzane są dane osobowe spełniały wymagania przewidziane przepisami o ochronie danych osobowych w przypadku nieskorzystania przez administratora danych z możliwości powołania administratora systemu informatycznego, pod wskazanym pojęciem rozumie się jednostkę organizacyjną właściwą w sprawach IT lub zewnętrzny podmiot zapewniający obsługę w zakresie funkcjonowania infrastruktury IT lub bezpośrednio administratora danych, w zakresie spraw związanych ze sprawnym funkcjonowaniem infrastruktury IT;
3. **Audyt** - „systematyczny, niezależny i udokumentowany proces uzyskiwania dowodów z audytu oraz jego obiektywnej oceny w celu określenia stopnia spełnienia kryteriów audytu" (PN-EN ISO 27000, pkt 2.5);
4. **Audytor** - osoba, która przeprowadza audyt;
5. **Audytowany** - organizacja, która jest audytowana;
6. **Autentyczność** - „właściwość, która polega na tym, że podmiot jest tym, za kogo się podaje" (PN-EN ISO 27000, pkt 2.8);
7. **Bezpieczeństwo danych osobowych** - zachowanie poufności, integralności i dostępności danych osobowych (art. 32 ust. 1 RODO);
8. **Dane biometryczne** - dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne (art. 4 pkt 14 RODO);
9. **Dane dotyczące zdrowia** - dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej - w tym o korzystaniu z usług opieki zdrowotnej - ujawniające informacje o stanie jej zdrowia (art. 4 pkt 15 RODO) ;
10. **Dane genetyczne -** dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej (motyw 34 RODO) ;
11. **Dane osobowe** - 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 (art. 4 pkt 11 RODO);
12. **Dostępność** - „właściwość bycia dostępnym i użytecznym na żądanie autoryzowanego podmiotu" (PN-EN ISO 27000, pkt 2.9);
13. **Dowód z audytu** - zapisy, stwierdzenia faktu lub inne informacje, które są istotne ze względu na kryteria audytu i możliwe do zweryfikowania (PN-EN ISO 19011);
14. **Działanie korygujące** - działanie w celu wyeliminowania przyczyny niezgodności i zapobieżeniu powtórzeniu;
15. **Ekspert techniczny** - osoba, która służy audytującemu specjalistyczną wiedzą lub umiejętnościami;

16. **Główna jednostka organizacyjna** - oznacza: a) jeżeli chodzi o administratora posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim - miejsce, w którym znajduje się jego centralna administracja w Unii, a jeżeli decyzje co do celów i sposobów przetwarzania danych osobowych zapadają w innej jednostce organizacyjnej tego administratora w Unii i ta jednostka organizacyjna ma prawo nakazać wykonanie takich decyzji, to za główną jednostkę organizacyjną uznaje się jednostkę organizacyjną, w której zapadają takie decyzje; b) jeżeli chodzi o podmiot przetwarzający posiadający jednostki organizacyjne w więcej niż jednym państwie członkowskim - miejsce, w którym znajduje się jego centralna administracja w Unii lub, w przypadku gdy podmiot przetwarzający nie ma centralnej administracji w Unii - jednostkę organizacyjną podmiotu przetwarzającego w Unii, w której odbywają się główne czynności przetwarzania w ramach działalności jednostki organizacyjnej podmiotu przetwarzającego, w zakresie w jakim podmiot przetwarzający podlega szczególnym obowiązkom na mocy niniejszego rozporządzenia;
17. **Grupa przedsiębiorstw** - przedsiębiorstwo sprawujące kontrolę oraz przedsiębiorstwa przez nie kontrolowane;
18. **Inspektor ochrony danych** - osoba wyznaczona przez administratora danych na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO;
19. **Integralność** - właściwość polegająca na zapewnieniu dokładności i kompletności;
20. **Kontrola dostępu** - środki mające na celu zapewnienie, że dostęp do aktywów jest autoryzowany i ograniczony w oparciu o wymagania biznesowe i wymagania bezpieczeństwa;
21. **Korekcja** - działanie w celu wyeliminowania wykrytej niezgodności;
22. **Kryteria audytu** - zestaw polityk, procedur lub wymagań używanych jako odniesienie, do których porównuje się dowody z audytu (PN-EN ISO 19011);
23. **Mający znaczenie dla sprawy i uzasadniony sprzeciw** - sprzeciw wobec projektu decyzji dotyczącej tego, czy doszło do naruszenia niniejszego rozporządzenia lub czy planowane działanie wobec administratora lub podmiotu przetwarzającego jest zgodne z niniejszym rozporządzeniem, który to sprzeciw musi jasno wskazywać wagę wynikającego z projektu decyzji ryzyka naruszenia podstawowych praw lub wolności osób, których dane dotyczą, oraz gdy ma to zastosowanie - wagę ryzyka zakłócenia swobodnego przepływu danych osobowych w Unii;
24. **Metoda doboru reprezentatywnych prób** - metoda audytowa stosowana w sytuacjach,
gdy ze względów praktycznych lub kosztowych nie jest możliwe analizowanie wszystkich informacji w trakcie audytu. Polega ona na zdefiniowaniu badanej zbiorowości, określeniu operatu losowania, ustaleniu liczebności próby, wyboru metody doboru próby oraz pobrania próby z określonego planu;
25. **Naruszenie ochrony danych osobowych (incydent)** - oznacza 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;
26. **Niezgodność** - niespełnienie wymagania;
27. **Odbiorca** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot , któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
28. **Ograniczenie przetwarzania** - oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
29. **Organ nadzorczy** - niezależny organ publiczny, ustanowiony przez państwo członkowskie Unii Europejskiej w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii Europejskiej
30. **Organizacja międzynarodowa** - organizacja i organy jej podlegające działające na podstawie prawa

międzynarodowego publicznego lub inny organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy;

31. **Plan audytu** - opis działań oraz ustaleń organizacyjnych związanych z audytem;
32. **Podmiot przetwarzający** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
33. **Polska norma** - norma PN-ISO/IEC 27002 Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady bezpieczeństwa informacji.
34. **Poufność** - właściwość polegająca na tym, że informacja nie jest udostępniana ani ujawniana nieautoryzowanym osobom, podmiotom lub procesom (PN-EN ISO 27000, pkt 2.12);
35. **Proces** - zbiór działań wzajemnie powiązanych oraz wzajemnie oddziałujących, które przekształcają wejścia w wyjścia;
36. **Profilowanie** - dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
37. **Program audytu** - ustalony zestaw audytów, jednego lub większej ich liczby, zaplanowanych w określonych ramach czasowych i mających określony cel;
38. **Przedsiębiorca** - osoba fizyczna lub prawna prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą;
39. **Przedstawiciel** - osoba fizyczna lub prawna mająca miejsce zamieszkania lub siedzibę w Unii, która została wyznaczona na piśmie przez administratora lub podmiot przetwarzający na mocy art. 27 do reprezentowania administratora lub podmiotu przetwarzającego w zakresie ich obowiązków wynikających z niniejszego rozporządzenia;
40. **Przetwarzanie**- operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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;
41. **Pseudonimizacja** - przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
42. **RODO** - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
43. **Ryzyko** - wpływ niepewności na cele;
44. **Strona trzecia** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które - z upoważnienia administratora lub podmiotu przetwarzającego - mogą przetwarzać dane osobowe;
45. **Transgraniczne przetwarzanie** - oznacza: a) przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności jednostek organizacyjnych w więcej, niż jednym państwie członkowskim administratora lub podmiotu przetwarzającego w Unii posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim; albo b)przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego w Unii, ale które znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim;
46. **Usługa społeczeństwa informacyjnego** - usługa w rozumieniu art. 1 ust. 1 lit. b) dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/1535 (1);

47. **Ustalenia z audytu** - wyniki oceny zebranych dowodów z audytu w stosunku do kryteriów audytu;
48. **Uwierzytelnianie** - pewność, że deklarowana charakterystyka podmiotu jest poprawna;
49. **Wiążące reguły korporacyjne** - polityki ochrony danych osobowych stosowane przez administratora lub podmiot przetwarzający, którzy posiadają jednostkę organizacyjną na terytorium państwa członkowskiego, przy jednorazowym lub wielokrotnym przekazaniu danych osobowych administratorowi lub podmiotowi przetwarzającemu w co najmniej jednym państwie trzecim w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą;
50. **Wniosek z audytu** - wyniki audytu po rozważeniu celów audytu i wszystkich ustaleń z audytu;
51. **Zabezpieczenie** - „środek, który modyfikuje ryzyko" (PN-EN ISO 27000, pkt 2.16);
52. **Zakres audytu** - obszar i granice audytu;
53. **Zdarzenie** - wystąpienie lub zmiana konkretnego zestawu okoliczności;
54. **Zespół audytujący** - jeden lub więcej audytorów przeprowadzających audyt, wspieranych przez ekspertów technicznych, jeżeli jest to wymagane;
55. **Zgoda osoby, której dane dotyczą** - dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
56. **Zgodność** - „spełnienie wymagania" (PN-EN ISO 27000, pkt 2.13).

USTALENIA METODOLOGICZNE:
CELE, ZAKRES, KRYTERIA, PODSTAWA AUDYTU

CEL

Celem oceny skutków dla ochrony danych było opisanie realizowanych przez organizację procesów przetwarzania danych osobowych oraz ocenienie ich konieczności i proporcjonalności, a także wspomożenie zarządzania ryzykiem naruszenia praw i wolności osób fizycznych wynikającym z przetwarzania danych osobowych poprzez ocenę ryzyka i określenie środków pozwalającym zaradzić tym czynnikom ryzyka

KRYTERIA

Ocena skutków dla ochrony danych (DPIA) oraz analiza ryzyka zostały przeprowadzone zgodnie z:

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
2. Wytyczną Grupy Art. 29 dotyczącej oceny skutków dla ochrony danych (WP 248);
3. ISO/IEC 29134 - Technika informacyjna - Techniki bezpieczeństwa - Wytyczne dla oceny skutków przetwarzania;
4. ISO/IEC 27005 - Technika informatyczna - Techniki bezpieczeństwa - Zarządzanie ryzykiem w bezpieczeństwie informacji;
5. ISO 31000 - Zarządzanie ryzykiem - Zasady i wytyczne.

ZAKRES

Ocena skutków dla ochrony danych oraz analiza ryzyka zostały przeprowadzone w odniesieniu do procesów przetwarzania, w stosunku do których badana organizacja stanowi administratora danych oraz w stosunku do zasobów, których badana organizacja jest właścicielem lub posiada uprawnienia do zarzadzania nimi.

OPIS METODYKI

Ocena skutków dla ochrony danych i analiza ryzyka zostały przeprowadzone z uwzględnieniem elementów określonych w RODO (art. 35 ust. 7 oraz motywy 84 i 90), tj.:

1. opisu planowanych operacji przetwarzania i celów przetwarzania;
2. oceny czy operacje przetwarzania są niezbędne oraz proporcjonalne;
3. oceny ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
4. oceny środków planowanych w celu:
    a. zaradzenia ryzyku;
    b. wykazania przestrzegania niniejszego rozporządzenia.

Kryteria, zgodnie z którymi zrealizowano ocenę skutków dla ochrony danych oraz analizę ryzyka obejmują następujące elementy:

1. systematyczny opis operacji przetwarzania (art. 35 ust. 7 lit. a RODO):
    a. uwzględniono charakter, zakres, kontekst i cele przetwarzania (motyw 90 RODO);
    b. w rejestrze zamieszczono dane osobowe, informacje o odbiorcach i okresie przechowywania danych osobowych;
    c. przedstawiono funkcjonalny opis operacji przetwarzania;
    d. zidentyfikowano zasoby, z którymi styczność mają dane osobowe (sprzęt komputerowy, oprogramowanie, sieci, osoby, opracowania lub kanały transmisji opracowań);
    e. uwzględniono przestrzeganie zatwierdzonych kodeksów postępowania (art. 35 ust. 8 RODO);
2. oceniono niezbędność oraz proporcjonalność (art. 35 ust. 7 lit. b RODO) poprzez wskazanie środków, których podjęcie jest planowane w celu zapewnienia przestrzegania rozporządzenia (art. 35 ust. 7 lit. d i motyw 90 RODO), uwzględniając:
    a. środki przyczyniające się do proporcjonalności i niezbędności przetwarzania z uwzględnieniem następujących aspektów:
        i. konkretne, wyraźne i prawnie uzasadnione cele (art. 5 ust. 1 lit. b RODO);
        ii. zgodność przetwarzania z prawem (art. 6 RODO);
        iii. dane adekwatne, stosowne oraz ograniczone do tego, co niezbędne do
        iv. celów, w których są przetwarzane (art. 5 ust. 1 lit. c RODO);
        v. ograniczony czas przechowywania (art. 5 ust. 1 lit. e RODO);
    b. środki przyczyniające się do zachowania praw osób, których dane dotyczą:
        i. poinformowanie osoby, której dane dotyczą (art. 12, 13 i 14 RODO);
        ii. prawo dostępu i prawo do przenoszenia danych (art. 15 i 20 RODO);
        iii. prawo do sprostowania i do usunięcia danych (art. 16, 17 i 19 RODO);
        iv. prawo do sprzeciwu i prawo do ograniczenia przetwarzania (art. 18, 19 i 21 RODO);
        v. relacje z podmiotem przetwarzającym (art. 28 RODO);
        vi. zabezpieczenia przy międzynarodowym przekazywaniu danych (rozdział V RODO);
        vii. uprzednie konsultacje (art. 36 RODO);
3. przeprowadzono działania w zakresie zarządzania ryzykiem naruszenia praw i wolności osób, których dane dotyczą (art. 35 ust. 7 lit. c RODO):
    a. uwzględniono źródło, charakter, specyfikę i powagę ryzyka (por. motyw 84 RODO), czy konkretniej, w przypadku każdego rodzaju ryzyka (bezprawnego dostępu, niepożądanej zmiany i zniknięcia danych), z punktu widzenia osób, których dane dotyczą:
        i. uwzględniono źródła ryzyka (motyw 90 RODO);
        ii. zidentyfikowano możliwe skutki dla praw i wolności osób, których dane dotyczą, w przypadku zdarzeń takich jak bezprawny dostęp, niepożądane zmiany i zniknięcie danych;
        iii. zidentyfikowano zagrożenia, które mogłyby doprowadzić do bezprawnego dostępu, niepożądanych zmian i zniknięcia danych;
        iv. oszacowano prawdopodobieństwo i powagę (motyw 90 RODO);
    b. określono środki, których podjęcie jest planowane w celu zaradzenia ryzyku (art. 35 ust. 7 lit. d i motyw 90 RODO);
4. zaangażowano zainteresowane strony:
    a. skonsultowano się z inspektorem ochrony danych w celu uzyskania zalecenia (art. 35 ust. 2 RODO);
    b. w stosownych przypadkach zasięgnięto opinii osób, których dane dotyczą, lub ich przedstawicieli (art. 35 ust. 9 RODO).

Prowadzenie oceny skutków dla ochrony danych jest procesem ciągłym, a nie jednorazowym. Oceną skutków dla ochrony danych należy objąć wszelkie operacje przetwarzania danych, w odniesieniu do których od czasu przeprowadzenia niniejszego DPIA zmieniły się warunki początkowe (zakres, cel, zgromadzone dane osobowe, tożsamość administratorów danych lub odbiorców, okres zatrzymywania danych, środki techniczne i organizacyjne itd.) i które mogą powodować wysokie ryzyko. Ponadto, przeprowadzenie oceny skutków dla ochrony danych może być wymagane po zmianie rodzaju ryzyka związanego z operacją przetwarzania, np. z powodu wykorzystania nowej technologii lub dlatego, że dane osobowe wykorzystywane są w innym celu.

USTALENIA KONTEKSTU PRZETWARZANIA

KONTEKST WEWNĘTRZNY ORAZ ZEWNĘTRZNY

Określenie zewnętrznego i wewnętrznego kontekstu organizacji było kluczowym czynnikiem dostosowania dalszych działań strategicznych, operacyjnych i technicznych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych. Analiza kontekstu pozwoliła ustalić co następuje:

Nazwa organizacji	PrzykładowaOrganizacja sp. z o.o.
Adres organizacji	ul. Kamionkowska 45 03-812 Warszawa
KONTEKST I PRZEGLĄD ORGANIZACJI	
PRZEGLĄD ORGANIZACJI	
Obszar działalności	Sprzedaż hurtowa żywności.
Krótki opis prowadzonej działalności lub kompetencji	Organizacja zajmuje się sprzedażą hurtową żywności, której nie jest producentem. Klienci - sklepy znajdują się na terenie kilku krajów Unii Europejskiej.
KONTEKST ZEWNĘTRZNY	
Jakie jest środowisko regulacyjne, w którym działa organizacja Źródło: art. 24 ust. 1 RODO, ISO 31010, pkt 4.3.3	Kodeks cywilny, ustawa o rachunkowości, ustawa o podatku dochodowym od osób prawnych. Kodeks pracy, ustawa o podatku dochodowym od osób fizycznych, Ordynacja podatkowa, ustawa o systemie ubezpieczeń społecznych.
KONTEKST WEWNĘTRZNY	

Jak wyglądają przepływy informacji i procesy decyzyjne? Źródło: (ISO 31010, pkt 4.3.3)	Audytowana organizacja wdrożyła zasady ładu korporacyjnego, obejmujące wszystkie komórki organizacyjne oraz szczeble decyzyjne, szczegółowo opisane w „Podziale kompetencji" oraz „Procedurze zarządzania projektami".
Proszę opisać zakres i granice zarządzania ryzykiem w ochronie danych osobowych. Źródło: (art.. 24 ust. 1 RODO, ISO 27005, pkt 7.3)	Zarządzanie ryzykiem w ochronie danych osobowych dotyczy wszystkich aktywów organizacji, które uczestniczą w procesach przetwarzania danych osobowych.

ANALIZA RYZYKA DLA PROCESÓW (DPIA)

Ocena skutków dla ochrony danych osobowych pozwoliła ustalić co następuje:

PROCES PRZETWARZANIA DANYCH W RAMACH SYSTEMU ZGŁASZANIA NARUSZEŃ PRZEZ SYGNALISTÓW

OCENA KONIECZNOŚCI PRZEPROWADZENIA DPIA	
Czy dochodzi do systematycznej, kompleksowej oceny czynników osobowych, opartej na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i będącej podstawą decyzji wywołujących skutki prawne lub w inny sposób znacząco wpływających na osobę fizyczną? Źródło: art. 35 ust. 3 lit. a RODO	Nie
Uzasadnij	Nie dochodzi do systematycznej, kompleksowej oceny czynników osobowych, opartej na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i będącej podstawą decyzji wywołujących skutki prawne lub w inny sposób znacząco wpływających na osobę fizyczną. W procesie zgłaszania naruszeń przez sygnalistów nie dokonuje się w ogóle oceny czynników osobowych, czy to samych sygnalistów, czy też potencjalnych sprawców naruszenia.
Czy dochodzi do przetwarzania na dużą skalę szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa? Źródło: art. 35 ust. 3 lit. b RODO	Nie
Uzasadnij	Nie dochodzi do przetwarzania na dużą skalę szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa. Sporadycznie jednak mogą się takie dane pojawić, w szczególności w odniesieniu do potencjalnego sprawcy naruszenia.
Czy dochodzi do systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie? Źródło: art. 35 ust. 3 lit. c RODO	Nie
Uzasadnij	Nie dochodzi do systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.
Czy organ nadzorczy uznał dany rodzaj operacji przetwarzania za podlegający wymogowi DPIA lub istnieją inne powody, dla których przetwarzanie z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych? Źródło: art. 35 ust. 1 i 4 RODO	Tak
Uzasadnij	Zgodnie z KOMUNIKATEM PREZESA URZĘDU OCHRONY DANYCH OSOBOWYCH z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony DPIA jest wymagane, gdy przetwarzanie spełnia co najmniej dwa ze wskazanych kryteriów. W procesie zgłaszania naruszeń przez sygnalistów spełnione jest kryterium 9. Przetwarzanie danych dotyczących osób, których ocena i świadczone im usługi są uzależnione od podmiotów lub osób, które dysponują uprawnieniami nadzorczymi i/lub ocennymi (Systemy służące do zgłaszania nieprawidłowości (whistleblowing)). Jedynie sporadycznie może dochodzić do sytuacji, gdy spełnione zostanie kryterium nr 4. Przetwarzanie szczególnych kategorii danych osobowych i dotyczących wyroków skazujących i czynów zabronionych (danych wrażliwych wg opinii WP 29). W ocenie Administratora istnieją też inne powody, dla których przetwarzanie z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, zarówno po stronie samego sygnalisty, jak i potencjalnego sprawcy naruszenia. W przypadku sygnalisty będzie to ryzyko jego napiętnowania w organizacji jako "konfidenta", zaś w przypadku potencjalnego sprawcy naruszenia - ryzyko napiętnowania takiej osoby jako naruszającej przepisy, jeszcze przed ostatecznym wyjaśnieniem sprawy i potwierdzeniem faktycznej sprawstwa.
Czy przetwarzanie łącznie:a) dotyczy danych zwykłych i jest niezbędne do wypełnienia obowiązku prawnego lub zadania realizowanego w interesie publicznym lub w ramach władzy publicznej?b) jest regulowane przepisami szczególnymi, dla których dokonano DPIA? Źródło: art. 35 ust. 10	Nie

Uzasadnij	Przetwarzanie dotyczy danych zwykłych (choć wynik postępowania może stanowić również dane osobowe dotyczące naruszeń prawa w myśl art. 10 RODO) i jest niezbędne do wypełnienia obowiązku prawnego. Przetwarzanie jest również regulowane przepisami szczególnymi, ale dla wskazanego przetwarzania nie dokonano DPIA.
Obowiązkowy DPIA	TAK
OPIS PROCESU I CELÓW PRZETWARZANIA	
PYTANIA OGÓLNE	
Cel przetwarzania danych	Celem przetwarzania jest realizacji przepisów ustawy z dnia …….. o ochronie osób zgłaszających naruszenia prawa, implementującej DYREKTYWĘ PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii.
Funkcjonalny opis operacji przetwarzania	Operacje przetwarzania danych osobowych dotyczą osób dokonujących zgłoszenia, zaś w stosownych przypadkach: - osób pomagających w dokonaniu zgłoszenia, - osób trzecich powiązanych z osobami dokonującymi zgłoszenia, które mogą doświadczyć działań odwetowych w kontekście związanym z pracą, takich jak współpracownicy lub krewni osób dokonujących zgłoszenia, - osób, których dotyczy zgłoszenie. Ustanowiono kanał wewnętrzny zgłaszania naruszeń, w ramach którego zgłoszenia przyjmuje się droga mailową (dedykowany mail sygnalista@organizacja.pl). Organizacja zatem nie dopuszcza dokonywania zgłoszeń w sposób całkowicie nie pozwalający na ustalenie tożsamości. Niemniej jednak dopuszczone jest zgłoszenie quasi-anonimowe, tj. zgłoszenie dokonane z dowolnego adresu mailowego oraz bez podawania imienia i nazwiska. W takim przypadku korespondencja z sygnalistą będzie prowadzona, niemniej jednak będzie się to odbywać w sposób uniemożliwiający nieuprawnione ujawnienie quasi-anonimowemu sygnaliście danych osobowych. Zgłoszenie jest rozpatrywane przez 3-osobową wewnętrzną komisję. Po otrzymaniu zgłoszenia komisja potwierdza jego otrzymanie drogą mailową. Dane są przechowywane w treści wiadomości mailowych, a także na wydzielonych zasobach na SharePoint (dostawca: Microsoft Ireland Operations Ltd), do których dostęp ma wyłącznie wspomniana komisja. Na zasobach znajdują się: dokumenty związane ze zgłoszeniem oraz plik Excel, stanowiący rejestr zgłoszeń. W rejestrze odnotowywane są: imię, nazwisko, e-mail, numer telefonu, stanowisko służbowe sygnalisty (jeśli znane), w przypadku zewnętrznych sygnalistów – dodatkowo firma, której sygnalista jest pracownikiem/współpracownikiem. Oprócz tego w rejestrze zamieszcza się krótki opis czego dotyczy zgłoszenie, data wysyłki potwierdzenia przyjęcia zgłoszenia, wynik postępowania, data powiadomienia sygnalisty o wyniku postępowania (wysyłki informacji zwrotnej). Procedury przewidują, że wszelka korespondencja z osobami, o których mowa wyżej, może odbywać się wyłącznie za pomocą dedykowanej skrzynki sygnalista@organizacja.pl. Okres przechowywania danych został ustalony na 5 lat od dnia przyjęcia zgłoszenia.
Czy uwzględniono przestrzeganie zatwierdzonych kodeksów postępowania?	Brak kodeksów postępowania, które mogłyby mieć zastosowanie.
Kategorie przetwarzanych danych osobowych "zwykłych"	Dane osoby dokonującej zgłoszenia: imię, nazwisko, stanowisko służbowe, adres e-mail, numer telefonu, w przypadku zewnętrznych sygnalistów – firma, wszelkie inne dane osobowe wynikające ze zgłoszenia. Dane osób pomagających w dokonaniu zgłoszenia - w zależności od kontekstu. Dane osób trzecich powiązanych z osobami dokonującymi zgłoszenia, które mogą doświadczyć działań odwetowych w kontekście związanym z pracą, takich jak współpracownicy lub krewni osób dokonujących zgłoszenia - w zależności od kontekstu. Dane osób, których dotyczy zgłoszenie - w zależności od kontekstu
Kategorie przetwarzanych danych osobowych szczególnej kategorii Źródło: art. 9 RODO RODO	W procesie nie przewiduje się przetwarzania danych szczególnych kategorii.
Kategorie przetwarzanych danych dotyczących wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa	Dane dotyczące wyroków skazujących oraz czynów zabronionych mogą pojawić się w treści zgłoszenia, jednak zależy to od kontekstu sprawy.
Kategorie podmiotów przetwarzających	Microsoft Ireland Operations Limited.
Kategorie podmiotów, którym dane zostały udostępnione	Organy publiczne, w szczególności organy wymiaru sprawiedliwości.
Planowane terminy usunięcia poszczególnych kategorii danych lub kryteria ich ustalenia	Okres usuwania danych został ustalony na 5 lat od dnia przyjęcia zgłoszenia.
NIEZBĘDNOŚĆ I PROPORCJONALNOŚĆ ORAZ ZAANGAŻOWANIE ZAINTERESOWANYCH STRON	
ZASADY PRZETWARZANIA DANYCH OSOBOWYCH	
Czy istnieją ważne podstawy prawne przetwarzania danych osobowych? Źródło: art. 6 ust. 1; art. 9 ust. 1	Art. 6 ust. 1 lit. c RODO w związku z ustawą z dnia …… o ochronie osób zgłaszających naruszenia prawa. Art. 6 ust. 1 lit. f RODO, tj. prawnie uzasadniony interes administratora w postaci dochodzenia lub obrony roszczeń.
Ocena zgodności	Zgodność
Rekomendacje (jak powinno być?)	

Czy osoba, której dane dotyczą, otrzymuje wszystkie wymagane informacje przy zbieraniu danych? Źródło: art. 13-14	Tak, procedura wewnętrznego zgłaszania naruszeń zamieszczona jest na stronie internetowej organizacji, gdzie znajdują się informacje na temat przetwarzania danych osób, których dane dotyczą. Link do procedury jest każdorazowo przesyłany w wiadomości zwrotnej po otrzymaniu zgłoszenia. Procedura realizacji obowiązku informacyjnego względem osób, których dotyczy naruszenie, zakłada rezygnację z jego realizacji w ściśle określonych sytuacjach, kiedy utrudniałoby to lub uniemożliwiało realizację celu ustawy (art. 14 ust. 5 lit. b RODO). Jednakże powody rezygnacji muszą być udokumentowane, zaś w momencie, kiedy ustanie powód rezygnacji ze spełnienia obowiązku informacyjnego, procedura przewiduje jego spełnienie.
Ocena zgodności	Zgodność
Rekomendacje (jak powinno być?)	
Czy dane są zbierane w konkretnym, wyraźnym i prawnie uzasadnionym celu? Czy dane nie są poddawane dalszemu przetwarzaniu niezgodnemu z tym celem? Źródło: art. 5 ust. 1 lit. b RODO	Dane są zbierane w konkretnym, wyraźnym i prawnie uzasadnionym celu – realizacji przepisów ustawy z dnia ..... o ochronie osób zgłaszających naruszenia prawa. Dane nie są poddawane dalszemu przetwarzaniu niezgodnemu z tym celem.
Ocena zgodności	Zgodność
Rekomendacje (jak powinno być?)	
Czy dane są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, dla których są przetwarzane? Źródło: art. 5 ust. 1 lit. c RODO	Dane są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, dla których są przetwarzane.
Ocena zgodności	Zgodność
Rekomendacje (jak powinno być?)	
Czy dane osobowe są 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? Źródło: art. 5 ust. 1 lit. e RODO	Dane osobowe są 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 – 5 lat od przyjęcia zgłoszenia.
Ocena zgodności	Zgodność
Rekomendacje (jak powinno być?)	
PRAWA OSOBY, KTÓREJ DANE DOTYCZĄ	
Czy osoba fizyczna może uzyskać: a) informację, czy dotyczące jej dane są przetwarzane, b) dostęp do tych danych, c) dostęp do informacji o przetwarzaniu, o których mowa w art. 15 ust. 1? Źródło: art. 15 ust. 1	Organizacja deklaruje możliwość zrealizowania wskazanych praw, z zastrzeżeniem wyjątków wskazanych w ustawie z dnia ..... o ochronie osób zgłaszających naruszenia prawa.
Ocena zgodności	Zgodność
Rekomendacje (jak powinno być?)	
Czy osoba fizyczna może uzyskać kopię dotyczących jej danych osobowych, zarówno w formie papierowej, jak i elektronicznej? Źródło: art. 15 ust. 3	Organizacja deklaruje możliwość zrealizowania wskazanego prawa, z zastrzeżeniem wyjątków wskazanych w ustawie z dnia ..... o ochronie osób zgłaszających naruszenia prawa.
Ocena zgodności	Zgodność
Rekomendacje (jak powinno być?)	
Czy osoba fizyczna może uzyskać w powszechnie używanym formacie elektronicznym dotyczące jej dane, które dostarczyła administratorowi? Źródło: art. 20	Z uwagi na brak spełnienia przesłanek, o których mowa w art. 20 RODO wskazane prawo nie jest realizowane.
Ocena zgodności	Zgodność
Rekomendacje (jak powinno być?)	
Czy osoba, której dane dotyczą może skorzystać z prawa do sprostowania danych?	Organizacja deklaruje możliwość zrealizowania wskazanego prawa.
Ocena zgodności	Zgodność

Rekomendacje (jak powinno być?)	
Czy osoba, której dane dotyczą, może skorzystać z prawa do usunięcia danych (do bycia zapomnianym)? Źródło: art. 17	Osoba, której dane dotyczą, może skorzystać z prawa do usunięcia danych (do bycia zapomnianym), jednakże pod warunkiem, że dane nie są już niezbędne dla realizacji celów wskazanych w ustawie lub dla dochodzenia bądź obrony roszczeń.
Ocena zgodności	Zgodność
Rekomendacje (jak powinno być?)	
Czy osoba, której dane dotyczą, może skorzystać z prawa do ograniczenia przetwarzania? Źródło: art. 18	Organizacja deklaruje możliwość zrealizowania wskazanego prawa.
Ocena zgodności	Zgodność
Rekomendacje (jak powinno być?)	
Czy osoba, której dane dotyczą, może skorzystać z prawa do sprzeciwu? Źródło: art. 21	Administrator nie przewiduje, żeby w przypadku przetwarzania danych na potrzeby dochodzenia lub obrony roszczeń osoba, której dane dotyczą, mogła złożyć skuteczny sprzeciw wobec przetwarzania jej danych.
Ocena zgodności	Zgodność
Rekomendacje (jak powinno być?)	
POWIERZENIE PRZETWARZANIA DANYCH	
Czy podmiot przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzane spełniało wymogi RODO? Źródło: art. 28 ust. 1 RODO	Microsoft Ireland Operations Ltd - umowa powierzenia (podpowierzenia) zawierana poprzez akceptację regulaminu usługi (https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?year=2021) i zawiera informacje na temat stosowanych przez Microsoft środków technicznych i organizacyjnych, spełniających wymogi RODO.
Ocena zgodności	Zgodność
Rekomendacje (jak powinno być?)	
Czy powierzenie przetwarzania danych osobowych odbywa się w granicach i na podstawie umowy lub instrumentu prawnego wymaganego przez RODO? Źródło: art. 28 ust. 3	Microsoft Ireland Operations Ltd - ze wskazanym podmiotem jest zawierana umowa powierzenia (podpowierzenia) poprzez akceptację regulaminu usługi (https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?year=2021).
Ocena zgodności	Zgodność
Rekomendacje (jak powinno być?)	
Czy podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego jedynie za uprzednią wiedzą i zgodą administratora? Źródło: art. 28 ust. 2	Microsoft Ireland Operations Ltd korzysta z usług innego podmiotu przetwarzającego jedynie za uprzednią wiedzą administratora, jednak faktycznie administrator nie ma wpływu na wybór podprocesora.
Ocena zgodności	Potencjalna niezgodność
Rekomendacje (jak powinno być?)	W razie zaangażowania przez Microsoft Ireland Operations Ltd podprocesora, który nie zapewnia gwarancji stosowania odpowiednich środków technicznych i organizacyjnych służących ochronie danych, należy zrezygnować z korzystania z usług Microsoft. Wymagane jest zatem monitorowanie wykazu podprocesorów zaangażowanych przez Microsoft.
Czy podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego na podstawie dokumentu prawidłowo określającego obowiązki stron? Źródło: art. 28 ust. 4	Tak, tak stanowi umowa powierzenia z Microsoft Ireland Operations Ltd.
Ocena zgodności	Zgodność
Rekomendacje (jak powinno być?)	
PRZEKAZYWANIE DANYCH POZA EUROPEJSKI OBSZAR GOSPODARCZY (EOG)	
Czy przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych odbywa się zgodnie z RODO? Źródło: art. 44-49	Nie zidentyfikowano przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych (w ramach usługi SharePoint).

Ocena zgodności	Nie dotyczy
Rekomendacje (jak powinno być?)	
W przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, proszę wskazać odpowiednie zabezpieczenia. Źródło: art. 49 ust. 1 akapit drugi RODO	Nie dotyczy – brak przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO.
Czy konsultowano ocenę skutków planowanych operacji przetwarzania dla ochrony danych osobowych z osobami, których dane dotyczą lub ich przedstawicielami?	Nie.
Czy konsultowano ocenę skutków planowanych operacji przetwarzania dla ochrony danych osobowych z inspektorem ochrony danych?	Tak.
RYZYKO NARUSZENIA PRAW I WOLNOŚCI OSÓB FIZYCZNYCH	
WSTĘP	
Jakie są zagrożenia, które mogłyby doprowadzić do bezprawnego dostępu, niepożądanych zmian i zniknięcia danych?	Bezprawny dostęp do danych, niepożądane zmiany czy zniknięcie danych może być związane z wygenerowaniem dostępu do zasobów na SharePoint dla wszystkich osób dysponujących linkiem (zamiast udostępnienie zasobu konkretnym osobom), a następnie nieprawidłowe przesłanie linku lub omyłkowe przeforwardowanie wiadomości z linkiem do nieuprawnionych osób.
Jakie są źródła zidentyfikowanych ryzyk?	Źródłem zidentyfikowanego w 5.1 ryzyka może być brak odpowiedniego zapisu w procedurze co do nadawania uprawnień do zasobów SharePoint.
JAKIE JEST RYZYKO KRADZIEŻY TOŻSAMOŚCI LUB OSZUSTWA DOTYCZĄCEGO TOŻSAMOŚCI?	
Uwzględniając powyżej wprowadzone informacje dotyczące procesu oceń wagę zagrożenia	Nie dotyczy
Uwzględniając powyżej wprowadzone informacje dotyczące procesu oceń prawdopodobieństwo wystąpienia zagrożenia	Nie dotyczy
JAKIE JEST RYZYKO NARUSZENIA ZAKAZU DYSKRYMINACJI?	
Uwzględniając powyżej wprowadzone informacje dotyczące procesu oceń wagę zagrożenia	3
Uwzględniając powyżej wprowadzone informacje dotyczące procesu oceń prawdopodobieństwo wystąpienia zagrożenia	2
JAKIE JEST RYZYKO SZKODY FINANSOWEJ DLA OSÓB, KTÓRYCH DANE DOTYCZĄ?	
Uwzględniając powyżej wprowadzone informacje dotyczące procesu oceń wagę zagrożenia	3
Uwzględniając powyżej wprowadzone informacje dotyczące procesu oceń prawdopodobieństwo wystąpienia zagrożenia	2
JAKIE JEST RYZYKO SZKODY WIZERUNKOWEJ DLA OSÓB, KTÓRYCH DANE DOTYCZĄ?	
Uwzględniając powyżej wprowadzone informacje dotyczące procesu oceń wagę zagrożenia	3
Uwzględniając powyżej wprowadzone informacje dotyczące procesu oceń prawdopodobieństwo wystąpienia zagrożenia	2
JAKIE JEST RYZYKO ZŁAMANIA TAJEMNICY ZAWODOWEJ, MAJĄCEJ CHRONIĆ OSOBY, KTÓRYCH DANE DOTYCZĄ?	
Uwzględniając powyżej wprowadzone informacje dotyczące procesu oceń wagę zagrożenia	Nie dotyczy
Uwzględniając powyżej wprowadzone informacje dotyczące procesu oceń prawdopodobieństwo wystąpienia zagrożenia	Nie dotyczy
WSZELKIE INNE NARUSZENIA PRAW I WOLNOŚCI OSÓB FIZYCZNYCH	

Uwzględniając powyżej wprowadzone informacje dotyczące procesu oceń wagę zagrożenia	Nie dotyczy
Uwzględniając powyżej wprowadzone informacje dotyczące procesu oceń prawdopodobieństwo wystąpienia zagrożenia	Nie dotyczy
WYMIEŃ ZIDENTYFIKOWANE PODATNOŚCI I WSKAŻ REKOMENDACJE	
Wymień zidentyfikowane podatności powodujące wysokie ryzyko dla naruszenia praw i wolności osób fizycznych	
Wskaż rekomendacje, których wdrożenie spowoduje, że zidentyfikowane ryzyko dla procesu będzie akceptowalne. W przypadku braku możliwości zminimalizowania ryzyka do poziomu akceptowalnego należy przeprowadzić uprzednie konsultacje z organem nadzorczym, o któ-rych mowa w art. 36 RODO.	

PLAN POSTĘPOWANIA Z RYZYKIEM PROCESÓW (DPIA)

Nie zidentyfikowano procesów przetwarzania danych osobowych powodujących wysokie ryzyko dla naruszenia praw i wolności osób fizycznych.

MAPA ZALEŻNOŚCI I POWIĄZAŃ

Podstawową funkcją mapy zależności i powiązań jest wskazanie, w których przetwarzania danych osobowych uczestniczą poszczególne zasoby zidentyfikowane na etapie „Inwentaryzacja zasobów".

Przeprowadzone działania pozwoliły na określenie następujących zasobów biorących udział w poszczególnych procesach przetwarzania:

#	Grupa zasobu	Nazwa zasobu	Powiązane procesy

ANALIZA RYZYKA DLA ZASOBÓW

Analiza ryzyka związanego z bezpieczeństwem zasobów uczestniczących w operacjach przetwarzania danych jest kolejnym krokiem do spełnienia obowiązku wynikającego z art. 32 ust. 1 RODO, tzn. wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przy przetwarzaniu danych osobowych zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych.

Ryzyko to wpływ niepewności na cele, ponieważ na realizację celów organizacji wpływa wiele nieznanych i zmiennych czynników. W odniesieniu do bezpieczeństwa zasobów uczestniczących w operacjach przetwarzania danych, poziom ryzyka stanowi kombinację prawdopodobieństw wystąpienia zdarzeń niepożądanych i ich konsekwencji.

Dzięki przeprowadzeniu analizy ryzyka było możliwe sformułowanie rekomendacji działań minimalizujących ryzyko dla poszczególnych zasobów. Przedmiotowe rekomendacje stanowią punkt wyjścia dla dostosowania środowiska teleinformatycznego do wymogów RODO.

Przeprowadzone działania pozwoliły na przedstawienie następujących wyników analizy ryzyka:

PLAN POSTĘPOWANIA Z RYZYKIEM ZASOBÓW

MOŻLIWE KONSEKWENCJE STWIERDZONYCH NIEZGODNOŚCI

Ustalone w trakcie audytu niezgodności mogą skutkować mierzalnymi lub/i niemierzalnymi konsekwencjami dla organizacji z tytułu uchybienia przepisom o ochronie danych osobowych.

Do możliwych mierzalnych (wyrażonych wprost w przepisach prawa) konsekwencji należy zaliczyć:

1. odpowiedzialność finansową w wysokości do 10 000 000 EUR lub 20 000 000 EUR, a w przypadku przedsiębiorstwa - w wysokości do 2 lub 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa,
2. wniesienie skargi do organu nadzorczego (Urzędu Ochrony Danych Osobowych),
3. odszkodowanie z tytułu majątkowej lub niemajątkowej szkody poniesionej przez osobę, której dane dotyczą,
4. odpowiedzialność karną z tytułu naruszenia przepisów o ochronie danych osobowych.

Do potencjalnych niemierzalnych konsekwencji należy zaliczyć:

1. utratę dobrego wizerunku,
2. szum medialny,
3. utratę części portfela klientów.

ZASADY MONITOROWANIA I PRZEGLĄDU

Oceny skutków dla ochrony danych należy dokonywać zawsze, gdy występuje możliwość zmiany ryzyka naruszenia praw lub wolności osób fizycznych. W ramach dobrych praktyk, oceny skutków dla ochrony danych należy dokonywać nie rzadziej niż raz w roku.