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

PrzykładowaOrganizacja sp. z o.o.

Fragment raportu
wygenerowany w wersji demonstracyjnej

Warszawa, 18.11.2020 r.

METRYKA DOKUMENTU

Wersja:	1.0	**Opis:**	Utworzenie pierwszej wersji dokumentu
Data sporządzenia:	2020-12-17		

Sporządził:	Damian Testowy	**Podpis:**	
Kontakt do audytora:	d.testowy@odo24.pl		

SPIS TREŚCI

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 rekrutacji
2. Proces przetwarzania danych pracowników/współpracowników
3. Proces dot. skarg i reklamacji
4. Proces przetwarzania danych klientów i ich przedstawicieli
5. Proces przetwarzania danych kontrahentów i ich przedstawicieli
6. Proces dochodzenia i obrony przed roszczeniami prawnymi
7. Proces przetwarzania danych w związku z prowadzoną księgowością
8. Proces dot. kontroli dostępu(monitoring wizyjny i rejestr wejść i wyjść)

Ponadto zdefiniowano następujące procesy przetwarzania danych, w stosunku do których organizacja jest podmiotem przetwarzającym (procesorem danych):

1. Proces pozyskiwania danych w imieniu ubezpieczyciela w ramach ubezpieczenia grupowego

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

1. Proces rekrutacji
2. Proces przetwarzania danych w związku z prowadzoną księgowością

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.

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	Branża farmaceutyczna
Krótki opis prowadzonej działalności lub kompetencji	Firma o zasięgu lokalnym, działająca na terytorium Polski, zatrudniająca 100 osób oraz zajmująca się produkcją i dystrybucją produktów XYZ
KONTEKST ZEWNĘTRZNY	
Jakie jest środowisko regulacyjne, w którym działa organizacja Źródło: art. 24 ust. 1 RODO, ISO 31010, pkt 4.3.3	Działalność jest oparta m.in.: o regulatory: Prawo Farmaceutyczne, Wytyczne i decyzje Głównego Inspektora Farmaceutycznego, Ustawa Refundacyjna, Wytyczne i rekomendacje Komisji Nadzoru Finansowego, Wyjaśnienia i wytyczne Prezesa Urzędu Ochrony Konkurencji i Konsumentów, Rozporządzenie Ministra Zdrowia w sprawie wymagań Dobrej Praktyki Wytwarzania, Rozporządzenie Ministra Zdrowia w sprawie wymagań Dobrej Praktyki Dystrybucyjnej, ustawa o bezpieczeństwie żywności i żywienia.

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.
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	Nie
Uzasadnij	Organ nadzorczy nie uznał danego rodzaju operacji przetwarzania za podlegający wymogowi DPIA i nie istnieją inne powody, dla których przetwarzanie z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.
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	Takie dane, w tym łącznie nie są przetwarzane w procesie.
Obowiązkowy DPIA	NIE
OPIS PROCESU I CELÓW PRZETWARZANIA	
PYTANIA OGÓLNE	

Cel przetwarzania danych	Audytowana organizacja pozyskuje dane klientów (reprezentantów osoby prawnej i ich pracowników) w wyraźnych i prawnie uzasadnionych celach jakim jest realizacja umowy bądź działania zmierzające do jej realizacji lub obrona/ dochodzenie roszczeń prawnych. Należy zaznaczyć, że dane członków zarządu reprezentujących osobę prawną, dane pełnomocników osób prawnych, a także dane pracowników, którzy są osobami kontaktowymi osoby prawnej, będących możliwymi do zidentyfikowania osobami fizycznymi, będą danymi osobowymi podlegającymi ochronie RODO (więcej: https://uodo.gov.pl/pl/225/1577). Również ochronie RODO podlegają dane osób prowadzących działalność gospodarczą, których dane ujawnione są w części jawnej CEiDG - co potwierdziła KE już w 2018 roku.
Funkcjonalny opis operacji przetwarzania	Kontakt telefoniczny lub elektroniczny (e-mail) z klientami (dystrybutorami lub aptekami) w celach realizacji umów.
Czy uwzględniono przestrzeganie zatwierdzonych kodeksów postępowania?	Brak zatwierdzonego kodeksu postępowania dla branży farmaceutycznej.
Kategorie przetwarzanych danych osobowych "zwykłych"	W przypadku pracowników klientów: imię i nazwisko, stanowisko, miejsce pracy, numer telefonu, adres e-mail. W przypadku klientów prowadzących działalność gospodarczą w formie jednoosobowej również miejsce wykonywania działalności, NIP, REGON.
Kategorie przetwarzanych danych osobowych szczególnej kategorii Źródło: art. 9 RODO RODO	Dane szczególnej kategorii nie są przetwarzane.
Kategorie przetwarzanych danych dotyczących wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa	Dane dot. wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa w procesie nie są przetwarzane.
Kategorie podmiotów przetwarzających	Dostawca usług hostingu poczty elektronicznej oraz dostawca systemu typu SAP. Dane są również powierzane podmiotowi świadczącemu usługi archiwizacji i utylizacji dokumentów.
Kategorie podmiotów, którym dane zostały udostępnione	Dane w procesie mogą być udostępnione podmiotom świadczącym usługi pocztowe lub kurierskie, jak również zewnętrznym kancelariom prawnym.

Planowane terminy usunięcia poszczególnych kategorii danych lub kryteria ich ustalenia	Dane osobowe będą przetwarzane przez okres do 6 lat od wykonania lub rozwiązania umowy. Po tym czasie dane zostaną usunięte.
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	Dane zwykłe przetwarzane są na podstawie art.. 6 ust. 1 lit b RODO - w przypadku gdy osoba fizyczna jest stroną umowy lub na podstawie art. 6 ust. 1 lit f RODO w przypadku gdy przetwarzane są dane reprezentantów osoby prawnej lub ich pracowników.
Ocena zgodności	Zgodność
Rekomendacje (jak powinno być?)	Brak rekomendacji.
Czy osoba, której dane dotyczą, otrzymuje wszystkie wymagane informacje przy zbieraniu danych? Źródło: art. 13-14	Audytowana organizacja nie spełnia obowiązku informacyjnego względem reprezentantów i pracowników klientów będących osobą prawną, jak również wobec klientów będących osobą fizyczną prowadzącą działalność gospodarczą w formie jednodobowej.
Ocena zgodności	Stwierdzona niezgodność
Rekomendacje (jak powinno być?)	Rekomenduje się wprowadzenie warstwowego obowiązku informacyjnego w stopkach mailowych wszystkich pracowników z odesłaniem do polityki prywatności, w której będą wskazane cele przetwarzania oraz będą zawarte inne informacje, o których mowa w art. 13 i 14 RODO. W przypadku zawierania umów w formie pisemnej rekomenduje się dodawanie zapisów dot. ochrony danych osobowych, w których będzie zobowiązanie do spełnienia obowiązku informacyjnego w imieniu audytowanej organizacji przez klienta będącego osobą prawną. Obowiązek informacyjny powinien być spełniony również wobec klientów będących osobą fizyczna prowadzącą działalność gospodarczą.

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	Audytowana organizacja deklaruje realizację praw osób, których dane dotyczą ale brak oficjalnych w tym zakresie procedur.
Ocena zgodności	Potencjalna niezgodność
Rekomendacje (jak powinno być?)	Rekomenduje się przyjęcie procedur realizacji praw osób, których dane dotyczą.
Czy osoba fizyczna może uzyskać kopię dotyczących jej danych osobowych, zarówno w formie papierowej, jak i elektronicznej? Źródło: art. 15 ust. 3	Osoba fizyczna może uzyskać kopię dotyczących jej danych osobowych, zarówno w formie papierowej, jak i elektronicznej, jednakże brak oficjalnych procedur w tym zakresie.
Ocena zgodności	Potencjalna niezgodność
Rekomendacje (jak powinno być?)	Rekomenduje się przyjęcie procedur realizacji praw osób, których dane dotyczą.
Czy osoba fizyczna może uzyskać w powszechnie używanym formacie elektronicznym dotyczące jej dane, które dostarczyła administratorowi? Źródło: art. 20	Osoba fizyczna będąca klientem może uzyskać w powszechnie używanym formacie elektronicznym dotyczące jej dane, które dostarczyła administratorowi, jednakże brak oficjalnych procedur w tym zakresie.
Ocena zgodności	Potencjalna niezgodność
Rekomendacje (jak powinno być?)	Rekomenduje się przyjęcie procedur realizacji praw osób, których dane dotyczą.
Czy osoba, której dane dotyczą może skorzystać z prawa do sprostowania danych?	Audytowana organizacja deklaruje, że w przypadku wniosku o sprostowanie, prawo zostałoby zrealizowane. Jednakże brak oficjalnych procedur w zakresie realizacji praw osób, których dane dotyczą.
Ocena zgodności	Potencjalna niezgodność
Rekomendacje (jak powinno być?)	Rekomenduje się przyjęcie procedur realizacji praw osób, których dane dotyczą.
Czy osoba, której dane dotyczą, może skorzystać z prawa do usunięcia danych (do bycia zapomnianym)? Źródło: art. 17	Audytowana organizacja deklaruje, że w przypadku wniosku o usuniecie danych - taki wniosek zostałby zweryfikowany pod kątem zasadności. Jednakże brak oficjalnych procedur w zakresie realizacji praw osób, których dane dotyczą.

Czy konsultowano ocenę skutków planowanych operacji przetwarzania dla ochrony danych osobowych z osobami, których dane dotyczą lub ich przedstawicielami?	Nie konsultowano ocenę skutków planowanych operacji przetwarzania dla ochrony danych osobowych z osobami, których dane dotyczą lub ich przedstawicielami.
Czy konsultowano ocenę skutków planowanych operacji przetwarzania dla ochrony danych osobowych z inspektorem ochrony danych?	Konsultowano ocenę skutków planowanych operacji przetwarzania dla ochrony danych osobowych z inspektorem ochrony danych.
RYZYKO NARUSZENIA PRAW I WOLNOŚCI OSÓB FIZYCZNYCH	
WSTĘP	
Jakie są zagrożenia, które mogłyby doprowadzić do bezprawnego dostępu, niepożądanych zmian i zniknięcia danych?	Zniszczenia fizyczne: pożar, zniszczenie,, utrata usług i awarie techniczne: awaria lub przeciążenie systemu/ urządzenia, utrata dostaw energii lub dostępu do sieci publicznej, naruszenie bezpieczeństwa informacji: podsłuch, kradzież, ujawnienie, szpiegostwo, nieautoryzowane działania: kopiowanie, przeglądanie, zmiana danych, nieautoryzowane użycie.
Jakie są źródła zidentyfikowanych ryzyk?	Występują mieszane źródła zidentyfikowanych ryzyk. Są to ryzyka mieszane: spowodowane czynnikami wewnętrznymi i zewnętrznymi.
JAKIE JEST RYZYKO KRADZIEŻY TOŻSAMOŚCI LUB OSZUSTWA DOTYCZĄCEGO TOŻSAMOŚCI?	
Uwzględniając powyżej wprowadzone informacje dotyczące procesu oceń wagę zagrożenia	2
Uwzględniając powyżej wprowadzone informacje dotyczące procesu oceń prawdopodobieństwo wystąpienia zagrożenia	2
JAKIE JEST RYZYKO NARUSZENIA ZAKAZU DYSKRYMINACJI?	
Uwzględniając powyżej wprowadzone informacje dotyczące procesu oceń wagę zagrożenia	1
Uwzględniając powyżej wprowadzone informacje dotyczące procesu oceń prawdopodobieństwo wystąpienia zagrożenia	1
JAKIE JEST RYZYKO SZKODY FINANSOWEJ DLA OSÓB, KTÓRYCH DANE DOTYCZĄ?	
Uwzględniając powyżej wprowadzone informacje dotyczące procesu oceń wagę zagrożenia	2

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
1.	Systemy operacyjne i aplikacje	SAP	Proces dot. skarg i reklamacji (ADO), Proces przetwarzania danych pracowników/współpracowników (ADO), Proces rekrutacji (ADO)
2.	Dokumenty w formie papierowej	Dokumenty zawierające dane księgowe	Proces rekrutacji (ADO)
3.	Dokumenty w formie papierowej	Dokumenty zawierające dane kadrowe	Proces dot. skarg i reklamacji (ADO)

IDENTYFIKOWANIE ZABEZPIECZEŃ	
Oceń poziom zabezpieczeń technicznych zasobu	2
Uzasadnij poziom zabezpieczeń technicznych zasobu	1. Ograniczone uprawnienia użytkowników oraz cykliczne ich przeglądy. 2. Dostęp do systemu realizowany z poziomu sieci WAN z wykorzystaniem protokołu TLS v. 1.3. 3. Polityka wymuszająca stosowanie haseł składających się z co najmniej 8 znaków, z czego małych, dużych liter, cyfr lub znaków specjalnych. Dodatkowo system wymusza zmianę haseł w cyklach kwartalnych oraz zapamiętuje 5 ostatnich wykorzystanych przez użytkownika poświadczeń logowania. 4. Zaimplementowane ograniczenia w zakresie możliwości uruchomienia w jednym czasie dwóch lub więcej sesji logowania na jednym identyfikatorze systemowym. 5. System utrzymywany w lokalnej serwerowni zapewniający wysoki poziom bezpieczeństwa fizycznego. 6. Cyklicznie wykonywanie kopii bezpieczeństwa. 7. Zastosowany system WAF oraz AV.
Oceń poziom zabezpieczeń organizacyjnych zasobu	2
Uzasadnij ocenę poziomu zabezpieczeń organizacyjnych zasobu	1. Szkolenia pracowników w zakresie obsługi systemu. 2. Cykliczne szkolenia pracowników dot. obowiązujących zasad bezpieczeństwa w organizacji. 3. Regulamin korzystania z systemów teleinformatycznych, którego zapoznanie i zobowiązanie do stosowania potwierdzane jest każdorazowo poprzez podpisanie stosowanego oświadczenia przez pracownika.
IDENTYFIKOWANIE PRAWDOPODOBIEŃSTWA WYSTĄPIENIA ZAGROŻEŃ	
Zniszczenia fizyczne Źródło: ISO 27005, załącznik C	3
Utrata usług i awarie techniczne Źródło: ISO 27005, załącznik C	3
Naruszenie bezpieczeństwa informacji Źródło: ISO 27005, załącznik C	3
Nieautoryzowane działania Źródło: ISO 27005, załącznik C	3

Naruszenie bezpieczeństwa funkcji Źródło: ISO 27005, załącznik C	1
OCENA EFEKTYWNOŚCI ZABEZPIECZEŃ	
Efektywność zabezpieczeń technicznych	1
Uzasadnienie - efektywność zabezpieczeń technicznych	1. Brak odporności systemu na ataki typu brute force 2. Brak zapewnienia wystarczającego poziomu bezpieczeństwa dla kopii zapasowych.
Efektywność zabezpieczeń organizacyjnych	1
Uzasadnienie - efektywność zabezpieczeń organizacyjnych	1. Brak weryfikacji przestrzegania przez pracowników organizacji przyjętych zasad bezpieczeństwa opisanych w funkcjonującym regulaminie
IDENTYFIKOWANIE PODATNOŚCI	
Opis podatności	1. Brak mechanizmu blokowania konta systemowego na wypadek kilkukrotnej próby logowania użytkownika z wykorzystaniem błędnego hasła. 2. Brak audytów weryfikujących sposób przestrzegania pracowników przyjętych w organizacji zasad bezpieczeństwa 3. Brak odseparowania fizycznego i logicznego wykonanych kopii bezpieczeństwa systemu SAP. 4. Podwyższone ryzyko zalania z powodu umieszczenia szafy rakowej z serwerami odpowiadającymi za utrzymanie systemu nad jednym z klimatyzatorów.
IDENTYFIKOWANIE NASTĘPSTW	
Wpływ na prawa i wolności osób, których dane dotyczą	5
Uzasadnienie - wpływ na prawa i wolności osób, których dane dotyczą	1. Wysokie ryzyko dyskryminacji osób, których dane dotyczą z powodu szerokiego zakresu danych dot. stanu zdrowia przetwarzanych w systemie
Poziom ryzyka (wynik analizy ryzyka)	29
Czy przekroczono próg akceptowalności?	TAK

Office 365

IDENTYFIKOWANIE ZABEZPIECZEŃ

Opis podatności	1. Brak wykreowanej osobnej sieci LAN dla systemów serwerowych
IDENTYFIKOWANIE NASTĘPSTW	
Wpływ na prawa i wolności osób, których dane dotyczą	5
Uzasadnienie - wpływ na prawa i wolności osób, których dane dotyczą	Katastrofalny wpływ na prawa i wolności.
Poziom ryzyka (wynik analizy ryzyka)	12
Czy przekroczono próg akceptowalności?	NIE

Windows 7

IDENTYFIKOWANIE ZABEZPIECZEŃ	
Oceń poziom zabezpieczeń technicznych zasobu	2
Uzasadnij poziom zabezpieczeń technicznych zasobu	1. Ograniczone uprawnienia użytkowników na poziomie OS. 2. Polityka wymuszająca stosowanie haseł składających się z co najmniej 8 znaków, z czego małych, dużych liter, cyfr lub znaków specjalnych. Dodatkowo system wymusza zmianę haseł w cyklach kwartalnych oraz zapamiętuje 5 ostatnich wykorzystanych przez użytkownika poświadczeń logowania. 3. System dołączony do Active Directory. 4. Wykonywane kopie bezpieczeństwa poszczególnych katalogów dysków lokalnych 5. Wdrożone wygaszacze ekranu blokujące konto systemowe po 5 minutach nieaktywności użytkownika.
Oceń poziom zabezpieczeń organizacyjnych zasobu	1
Uzasadnij ocenę poziomu zabezpieczeń organizacyjnych zasobu	1. Brak zabezpieczeń organizacyjnych
IDENTYFIKOWANIE PRAWDOPODOBIEŃSTWA WYSTĄPIENIA ZAGROŻEŃ	
Zniszczenia fizyczne Źródło: ISO 27005, załącznik C	0
Utrata usług i awarie techniczne Źródło: ISO 27005, załącznik C	4

Naruszenie bezpieczeństwa informacji Źródło: ISO 27005, załącznik C	4
Nieautoryzowane działania Źródło: ISO 27005, załącznik C	4
Naruszenie bezpieczeństwa funkcji Źródło: ISO 27005, załącznik C	4
OCENA EFEKTYWNOŚCI ZABEZPIECZEŃ	
Efektywność zabezpieczeń technicznych	1
Uzasadnienie - efektywność zabezpieczeń technicznych	1. Zabezpieczenia nie są skuteczne z powodu braku aktualizacji systemowych publikowanych przez Microsoft.
Efektywność zabezpieczeń organizacyjnych	1
Uzasadnienie - efektywność zabezpieczeń organizacyjnych	1. Zabezpieczenia nie są testowane i nie są skuteczne.
IDENTYFIKOWANIE PODATNOŚCI	
Opis podatności	1. System pozbawiony jest wsparcia producenta.
IDENTYFIKOWANIE NASTĘPSTW	
Wpływ na prawa i wolności osób, których dane dotyczą	5
Uzasadnienie - wpływ na prawa i wolności osób, których dane dotyczą	Katastrofalny wpływ na prawa i wolności ze względu na zakres i skalę przetwarzanych danych osobowych z wykorzystaniem systemu
Poziom ryzyka (wynik analizy ryzyka)	27
Czy przekroczono próg akceptowalności?	TAK

GRUPA: SPRZĘT BIUROWY (OGÓLNODOSTĘPNY)

Urządzenia wielofunkcyjne

IDENTYFIKOWANIE ZABEZPIECZEŃ	
Oceń poziom zabezpieczeń technicznych zasobu	2

PLAN POSTĘPOWANIA Z RYZYKIEM ZASOBÓW

Wyniki przeprowadzonej analizy ryzyka dla zasobów pozwoliły ustalić co następuje:

GRUPA: SYSTEMY OPERACYJNE I APLIKACJE

SAP

Poziom ryzyka	29
Zidentyfikowane podatności	1. Brak mechanizmu blokowania konta systemowego na wypadek kilkukrotnej próby logowania użytkownika z wykorzystaniem błędnego hasła. 2. Brak audytów weryfikujących sposób przestrzegania pracowników przyjętych w organizacji zasad bezpieczeństwa 3. Brak odseparowania fizycznego i logicznego wykonanych kopii bezpieczeństwa systemu SAP. 4. Podwyższone ryzyko zalania z powodu umieszczenia szafy rakowej z serwerami odpowiadającymi za utrzymanie systemu nad jednym z klimatyzatorów.
Rodzaj reakcji na ryzyko	Redukcja
Rekomendowane działania minimalizujące ryzyko	1. Podwyższenie bezpieczeństwa logowania do systemu poprzez wdrożenie mechanizmu blokowania systemowego użytkownika na wypadek 3-krotnej próby wprowadzenia błędnych poświadczeń logowania lub wdrożenie MFA. 2. Cykliczne, nie rzadziej niż raz w roku wykonywanie audytów weryfikujących sposób przestrzegania przez pracowników wewnętrznych procedur bezpieczeństwa. 3. Skonfigurowanie replikacji kopii zapasowych do serwerowni zapasowej. 4. Zmiana miejsca usytuowania szafy rakowej z serwerami odpowiadającymi za utrzymanie systemu.
Planowana data wykonania zadania	2021-07-31
Osoba odpowiedzialna	Marcin Odowski

Windows 7

Poziom ryzyka	27
Zidentyfikowane podatności	1. System pozbawiony jest wsparcia producenta.

Rodzaj reakcji na ryzyko	Unikanie
Rekomendowane działania minimalizujące ryzyko	1. Należy podnieść wersję niewspieranego przez producenta systemu
Planowana data wykonania zadania	2021-03-31
Osoba odpowiedzialna	Jan Kowalski

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.