Raport zgodności z RODO

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:	2020-11-25		

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

SPIS TREŚCI

WNIOSKI Z AUDYTU

Celem audytu było określenie poziomu zgodności przetwarzania danych osobowych przez PrzykładowaOrganizacja sp. z o.o. z przepisami europejskiego rozporządzenia o ochronie danych osobowych (RODO).

Wskazany powyżej cel audytu został zrealizowany. w na podstawie przeprowadzonego audytu ustalono, że organizacja PrzykładowaOrganizacja sp. z o.o. jest zgodna w 56% z postanowieniami RODO.

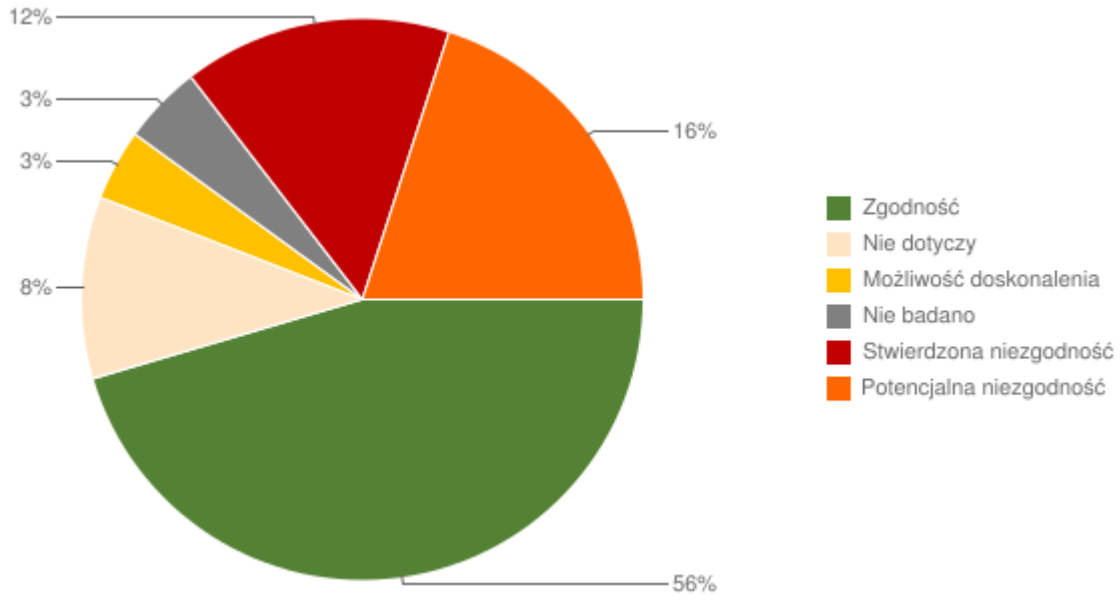
Poziom zgodności zweryfikowanych obszarów z przyjętymi kryteriami przedstawia się następująco:

1. Analiza wypełniania obowiązków przez ADO 40%
2. Analiza procesów (ADO) 62%
3. Analiza procesów (PP) 0%
4. Analiza zabezpieczeń 44%

Na podstawie przeprowadzonych działań zidentyfikowano:

1. 154 zgodności - stwierdzono zgodność z wymogiem
2. 23 nie dotyczy – stwierdzono wyłączenie danego kryterium z badania
3. 9 możliwości doskonalenia - stwierdzono zgodność z wymogiem, ale zaleca się wdrożenie bardziej efektywnych rozwiązań
4. 10 nie badano – nie zweryfikowano obszaru lub nie wystarczającą ilość informacji do jego oceny
5. 34 niezgodności – stwierdzono niezgodność z wymogiem
6. 44 potencjalnych niezgodności - stwierdzono zgodność z wymogiem, ale istnieje zagrożenie, które w przyszłości może skutkować niezgodnością lub incydentem

Poniższa grafika obrazuje stopień spełnienia przez badaną organizację przyjętych w danym obszarze kryteriów audytu:



Legenda:

	zgodności - stwierdzono zgodność z wymogiem
	możliwości doskonalenia - stwierdzono zgodność z wymogiem, ale zaleca się wdrożenie bardziej efektywnych rozwiązań
	potencjalnych niezgodności - stwierdzono zgodność z wymogiem, ale istnieje zagrożenie, które w przyszłości może skutkować niezgodnością lub incydentem
	niezgodności – stwierdzono niezgodność z wymogiem
	nie dotyczy – stwierdzono wyłączenie danego kryterium z badania
	nie badano – nie zweryfikowano obszaru lub nie wystarczającą ilość informacji do jego oceny

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;

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);

USTALENIA METODOLOGICZNE: CELE, ZAKRES, KRYTERIA, PODSTAWA AUDYTU

Audyt miał charakter audytu pierwszej strony, tj. został wykonany przez audytorów określonych w wykazie zamieszczonym w dalszej części raportu. Przeprowadzone działania miały za zadanie w sposób obiektywny sformułować opinię dotyczącą funkcjonującego systemu ochrony danych osobowych w kontekście spełnienia wymagań RODO.

Audyt został przeprowadzony z uwzględnieniem zasad określonych w normie PN-EN ISO 19011 Wytyczne dotyczące audytowania systemów zarządzania.

CEL AUDYTU

Celem audytu było określenie poziomu zgodności przetwarzania danych osobowych przez administratora danych z przepisami europejskiego rozporządzenia o ochronie danych osobowych (RODO).

KRYTERIA AUDYTU

Przyjęte kryteria audytu obejmują następujące wymagania:

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. Wytyczne Grupy Art. 29 dotyczące inspektorów ochrony danych (WP 243);
3. Wytyczne Grupy Art. 29 dotyczące prawa do przenoszenia danych (WP 242);
4. Wytyczne Grupy Art. 29 dotyczące ustalenia wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego (WP 244);
5. Wytyczne Grupy Art. 29 dotyczące oceny skutków dla ochrony danych (WP 248);
6. Norma PN-ISO/IEC 27002 Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady bezpieczeństwa informacji (wybrane zagadnienia wskazane w treści raportu);
7. Norma PN-ISO/IEC 27017 Technika informatyczna - Techniki bezpieczeństwa - Kodeks postępowania w zakresie kontroli bezpieczeństwa dla usług chmury (wybrane zagadnienia wskazane w treści raportu).

ZAKRES AUDYTU

Zakres audytu wyznaczył funkcjonujący system ochrony danych osobowych. w ramach audytu poddano weryfikacji następujące elementy:

1. analiza wypełniania obowiązków administratora danych wynikających z RODO,
2. analiza procesów przetwarzania danych osobowych, w stosunku do których organizacja jest administratorem danych, w zakresie zgodności z:
    a. zasadami przetwarzania danych osobowych,
    b. przetwarzania z prawem,
    c. obowiązkiem przejrzystego informowania i przejrzystej komunikacji oraz tryb wykonywania praw przez osobę,

której dane dotyczą,
   d. realizacji obowiązku informacyjnego,
   e. realizacji prawa umożliwienia dostępu do danych osobowych osobie, której dane dotyczą,
   f. dopełnieniem względem osób, których dane dotyczą obowiązku informacyjnego,
   g. realizacją prawa sprostowania i usuwania danych,
   h. realizacji prawa do ograniczenia przetwarzania,
   i. realizacji prawa do przenoszenia danych,
   j. realizacji prawa do sprzeciwu oraz zasad zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach,
   k. uregulowaniem powierzania danych do przetwarzania,
   l. zasadami dotyczącymi zabezpieczenia danych osobowych (w tym m.in. realizowanie przez Zleceniodawcę obowiązku regularnego testowania, mierzenia i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania) ,
   m. zasadami przekazywania danych do państw trzecich lub organizacji międzynarodowych,
   n. uwzględniania ochrony danych w fazie projektowania oraz ich domyślnej ochrony,
   o. rejestrowania czynności przetwarzania,
   p. przetwarzania danych z upoważnienia administratora danych,
3. analiza procesów przetwarzania danych osobowych, w stosunku do których organizacja jest podmiotem przetwarzającym (procesorem danych),
4. analiza stosowanych przez organizację technicznych i organizacyjnych środków ochrony danych osobowych, w zakresie:
   a. adekwatności stosowanych zabezpieczeń,
   b. pseudonimizacji i szyfrowania danych osobowych,
   c. zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego
   d. regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania
   e. zdolności do zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania.

OPIS METODYKI AUDYTU

Przeprowadzony audyt stanowił systematyczny, niezależny i udokumentowany proces mający na celu uzyskanie dowodów z audytu i dokonania ich obiektywnej oceny w celu określenia stopnia spełnienia kryteriów audytu.

Główną metodą gromadzenia dowodów audytowych był wywiad osobowy połączony z weryfikacją powziętych informacji podczas przeprowadzonej wizji lokalnej wybranych pomieszczeń tworzących obszar przetwarzania danych osobowych.

Dodatkowymi metodami badawczymi były:

- analiza przekazanej dokumentacji,
- analiza stron internetowych oraz oficjalnych profili na portalach społecznościowych należących do administratora danych,
- weryfikacja funkcjonalności systemów informatycznych służących do przetwarzania danych osobowych wykorzystywanych przez administratora danych.

Ponieważ audyt został przeprowadzony z wykorzystaniem metody doboru reprezentatywnych prób, możliwą jest sytuacja,

WYNIKI PRZEPROWADZONEGO AUDYTU

USTALENIA OGÓLNE ORAZ INFORMACJE O ORGANIZACJI

Audytowana organizacja stanowi klasyczny system otwarty, w którym informacje (dane osobowe) wpływają do niej (m.in. podczas procesu rekrutacji), są przez nią przetwarzane (m.in. poprzez przechowywanie, archiwizowanie, opracowywanie, zmienianie, usuwanie) oraz przekazywane na zewnątrz organizacji (np. uprawnionym organom Państwa, ubezpieczycielom, urzędom skarbowym, podmiotom służby zdrowia).

Analizie poddano zidentyfikowane procesy pozyskiwania danych osobowych (ustalenie podstaw prawnych przetwarzania, dopełnienie obowiązku informacyjnego), przetwarzania danych osobowych w ramach organizacji (adekwatność stosowanych technicznych i organizacyjnych środków ochrony danych) oraz przekazywania ich poza organizację (powierzenie przetwarzania, przekazywanie danych do państwa trzeciego).

Rys. 1 Przykładowy model przepływu danych osobowych w audytowanej organizacji

OBSZAR NR I
ANALIZA WYPEŁNIANIA OBOWIĄZKÓW ADMINISTRATORA DANYCH WYNIKAJĄCYCH Z RODO

USTALENIA AUDYTOWE

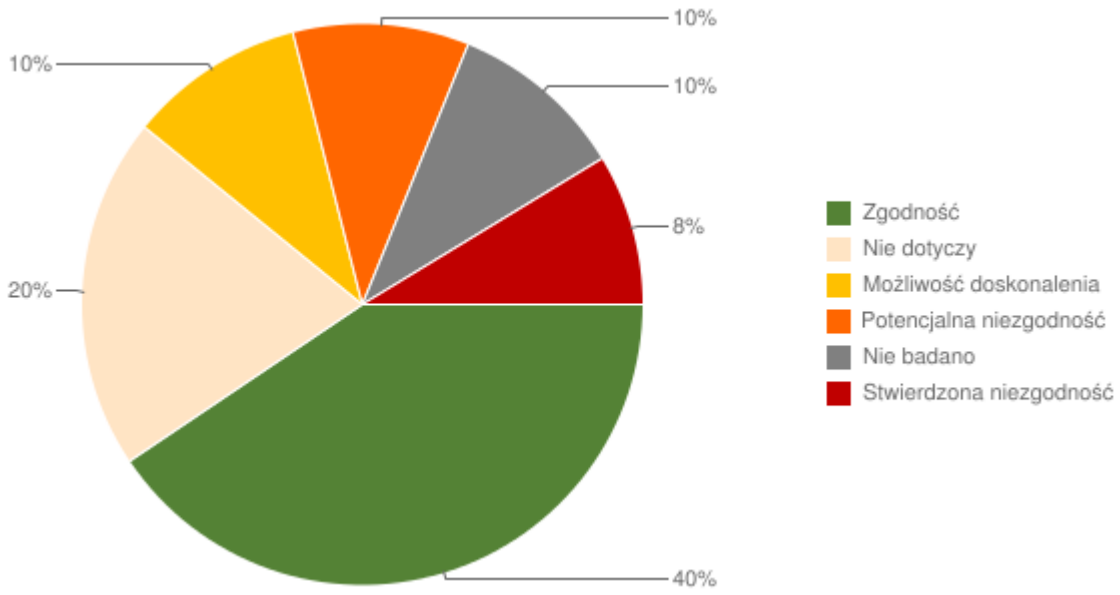
Analiza spełnienia przez organizację nałożonych na nią w badanym obszarze obowiązków pozwoliła ustalić, co następuje

INSPEKTOR OCHRONY DANYCH (IOD)			
Pytanie i jego źródło w RODO	Odpowiedź (jak jest?)	Stopień zgodności	Rekomendacje (jak powinno być?)
Czy spełniono obowiązek wyznaczenia IOD? Źródło: art. 37 ust. 1 RODO, art. 46 ust. 1 Ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości	Audytowana organizacja wyznaczyła fakultatywnie IOD - Uchwała Zarządu z dnia 4 listopada 2019 roku.	Zgodność	Brak rekomendacji. Audytowana organizacja, to firma z branży farmaceutycznej o zasięgu lokalnym, w związku z powyższym nie można mówić o przetwarzaniu danych szczególnej kategorii na dużą skalę w kontekście art. 37 ust. 1 lit c RODO. Jednakże zespół audytowy pozytywnie ocenia fakt wyznaczenia IOD, którego zadaniem jest sprawowanie pieczy nad systemem ochrony danych.
Czy IOD został wyznaczony na podstawie kwalifikacji zawodowych, fachowej wiedzy na temat prawa i praktyk w dziedzinie ochrony danych osobowych oraz umiejętności wypełniania zadań wynikających z RODO? Źródło: art. 37 ust. 5 RODO	IOD jest kierownik działu personalnego audytowanej organizacji. Zespół audytowy po rozmowie z wyznaczonym IOD ma zastrzeże co do fachowej wiedzy na temat prawa i praktyk w dziedzinie ochrony danych osobowych oraz umiejętności wypełniania zadań wynikających z RODO.	Potencjalna niezgodność	Rekomenduje się zobowiązać wyznaczonego IOD do podniesienia wiedzy z zakresu ochrony danych osobowych, w tym kwalifikacji zawodowych.
Czy łatwo jest skontaktować się z IOD z każdej jednostki organizacyjnej? Źródło: art. 37 ust. 2 RODO	123	Nie dotyczy	Brak rekomendacji.

Czy dane kontaktowe IOD zostały opublikowane i terminowo zawiadomiono o nich organ nadzorczy? Źródło: art. 37 ust. 7 RODO, art. 10 i 11 Ustawy o ochronie danych osobowych	Audytowana organizacja terminowo zawiadomiła Prezesa UODO o wyznaczeniu IOD, jednakże nie opublikowała na stronie internetowej imienia i nazwiska IOD oraz adresu e-mail lub numeru telefonu. (vide: art. 10 i 11 Ustawy o ochronie danych osobowych)	Stwierdzona niezgodność	Rekomenduje się niezwłocznie opublikować na stronie internetowej audytowanej organizacji w zakładce kontakt informacji o wyznaczeniu IOD wraz z imieniem i nazwiskiem oraz z uwagi na rozliczność ewentualnych kontaktów z IOD adres e-mail IOD.
Czy IOD jest włączany we wszystkie sprawy dotyczące ochrony danych osobowych, posiada zasoby niezbędne do wykonania swoich zadań i utrzymania wiedzy fachowej, a także ma dostęp do danych osobowych i operacji przetwarzania? Źródło: art. 38 ust. 1 i 2	Administrator deklaruje, żeIOD jest włączany we wszystkie sprawy dotyczące ochrony danych osobowych, posiada zasoby niezbędne do wykonania swoich zadań i utrzymania wiedzy fachowej. Jednakże w ocenie zespołu audytowego wyznaczony IOD powinien brać udział w spotkaniach roboczych średniego szczebla menadżerskiego celem posiadania bieżącej wiedzy o prowadzonych działaniach i projektach.	Potencjalna niezgodność	Rekomenduje się zapraszać IOD na spotkania robocze średniego szczebla menadżerskiego.
Czy IOD nie otrzymuje instrukcji dotyczących swoich zadań, podlega bezpośrednio najwyższemu kierownictwu oraz nie jest odwoływany ani karany za wypełnianie swoich zadań? Źródło: art. 38 ust. 3 RODO	IOD nie otrzymuje instrukcji dotyczących swoich zadań, podlega bezpośrednio najwyższemu kierownictwu.	Zgodność	Brak rekomendacji.
Czy inne zadania i obowiązki, które wykonuje IOD, nie powodują konfliktu interesów? Źródło: art. 38 ust. 6 RODO	Wyznaczony IOD jest również kierownikiem działu personalnego, co w ocenie zespołu audytowego powoduje konflikt interesów.	Stwierdzona niezgodność	IOD może wykonywać inne zadania w organizacji ale zadanie te nie mogą powodować konfliktu interesów. Rekomenduje się wyznaczyć innego IOD.

REKOMENDACJE POAUDYTOWE

Poniższa grafika obrazuje procentowy stopień spełnienia przez badaną organizację przyjętych kryteriów audytu:



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	Organ nadzorczy nie uznał danego rodzaju operacji przetwarzania za podlegający wymogowi DPIA.
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	Kryterium nie jest spełnione.
Obowiązkowe DPIA?		NIE

PROCES: PROCES PRZETWARZANIA DANYCH KLIENTÓW I ICH PRZEDSTAWICIELI

OPIS PROCESU I CELÓW PRZETWARZANIA	
PYTANIA OGÓLNE	
Lokalizacja procesu	Proces zlokalizowany jest w siedzibie administratora.
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.

Znaczenie procesu przetwarzania danych dla realizacji zadań biznesowych	Kluczowe
Kategorie osób, których dane dotyczą	Pracownicy klientów lub klienci prowadzący działalność gospodarczą w formie jednoosobowej.
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 osób działających z upoważnienia administratora i mające dostęp do danych osobowych	Dostęp do danych mają upoważnieni pracownicy działu handlowego, księgowego i prawnego.
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.
Zakres danych osobowych przekazywanych do państwa trzeciego lub organizacji międzynarodowej oraz nazwa tego państwa trzeciego lub organizacji międzynarodowej	Dane przetwarzane są na ternie EOG.
Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa	Dane w formie papierowej przechowywane są w zamykanych szafach, do których dostęp posiadają pracownicy działu kadr. Dane w formie elektronicznej przechowywane są na komputerach pracowników. Komputery te zabezpieczone są szyfrowaniem dysku, hasłem do systemu oraz programem antywirusowym.
W przypadku współadministrowania - nazwy oraz dane kontaktowe wszelkich współadministratorów Źródło: art. 26 ust. 1 RODO	Dane nie są współadministrowane.
W przypadku współadministrowania - podział kompetencji w zakresie przetwarzania danych	Dane nie są współadministrowane.

Stopień poufności danych przetwarzanych w ramach procesu	Poufne

NIEZBĘDNOŚĆ I PROPORCJONALNOŚĆ ORAZ ZAANGAŻOWANIE ZAINTERESOWANYCH STRON

ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

Pytanie i jego źródło w RODO	Odpowiedź (jak jest?)	Stopień zgodności	Rekomendacje (jak powinno być?)
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.	Zgodność	Brak rekomendacji.
Czy dane osobowe przetwarzane są wyłącznie na polecenie administratora? Czy nadawane są upoważnienia? Źródło: art. 29 RODO	Audytowana organizacja nadaje upoważnienia do przetwarzania danych w formie elektronicznej.	Zgodność	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.	Stwierdzona niezgodność	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 wymagane informacje są udzielane terminowo? Źródło: art. 12-14	Obowiązek informacyjny nie jest w ogóle spełniany.	Stwierdzona niezgodność	Rekomenduje się spełnianie obowiązku informacyjnego.

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.	Zgodność	Brak rekomendacji.
Czy domyślnie przetwarzane są wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania? Źródło: art. 25 ust. 2	Domyślnie przetwarzane są wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania.	Zgodność	Brak rekomendacji.
Czy jest weryfikowana prawidłowość danych, a w razie potrzeby dane są uaktualniane? Źródło: art. 5 ust. 1 lit. d	Audytowana organizacja nie ma przyjętych procedur w tym zakresie.	Potencjalna niezgodność	Rekomenduje się przyjęcie procedur weryfikowana prawidłowość danych.
Czy podejmowane są wszelkie rozsądne działania, aby dane które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane? Źródło: art. 5 ust. 1 lit. d, art. 16	Audytowana organizacja deklaruje, że podejmowane są wszelkie rozsądne działania, aby dane które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane. Jednakże brak oficjalnych procedur w zakresie realizacji praw osób, których dane dotyczą.	Stwierdzona niezgodność	Rekomenduje się przyjęcie procedur realizacji praw osób, których dane dotyczą.
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.	Zgodność	Brak rekomendacji.

Czy administrator jest w stanie wykazać przestrzeganie zasad przetwarzania danych osobowych? Źródło: art. 5 ust. 2	Audytowana organizacja nie jest w stanie wykazać przestrzeganie zasad przetwarzania danych osobowych, ponieważ nie realizuje wszystkich zasad przetwarzania danych.	Stwierdzona niezgodność	Rekomenduje się przestrzeganie wszystkich zasad, o których mowa w art. 5 RODO.
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	Audytowana organizacja deklaruje realizację praw osób, których dane dotyczą ale brak oficjalnych w tym zakresie procedur.	Potencjalna niezgodność	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.	Potencjalna niezgodność	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.	Potencjalna niezgodność	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.	Potencjalna niezgodność	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.	Potencjalna niezgodność	Rekomenduje się przyjęcie procedur realizacji praw osób, których dane dotyczą.
Czy osoba, której dane dotyczą, może skorzystać z prawa do ograniczenia przetwarzania? Źródło: art. 18	Audytowana organizacja deklaruje, że w przypadku wniosku o ograniczenie przetwarzania - taki wniosek zostałby zweryfikowany pod kątem zasadności. Jednakże brak oficjalnych procedur w zakresie realizacji praw osób, których dane dotyczą.	Potencjalna niezgodność	Rekomenduje się przyjęcie procedur realizacji praw osób, których dane dotyczą.
Czy odbiorcy są informowani o sprostowaniu, usunięciu lub ograniczeniu przetwarzania ujawnionych im danych osobowych? Źródło: art. 19	Brak oficjalnych procedur w tym zakresie.	Stwierdzona niezgodność	Rekomenduje się przyjęcie procedur informowania odbiorcy są informowani o sprostowaniu, usunięciu lub ograniczeniu przetwarzania ujawnionych im danych osobowych.

Czy osoba, której dane dotyczą, może skorzystać z prawa do sprzeciwu? Źródło: art. 21	Audytowana organizacja deklaruje, że w przypadku wniosku o sprostowanie, prawo zostałoby zrealizowane. Jednakże brak oficjalnych procedur w zakresie realizacji praw osób, których dane dotyczą. Sprzeciw może zostać zrealizowany w sytuacji gdy przetwarzanie danych odbywa się na podstawie art. 6 ust. 1 lit f RODO.	Potencjalna niezgodność	Rekomenduje się przyjęcie procedur realizacji praw osób, których dane dotyczą.
Czy zautomatyzowane podejmowanie decyzji wobec osoby, której dane dotyczą, odbywa się zgodnie z RODO? Źródło: art. 22	W procesie nie są podejmowane zautomatyzowane decyzje.	Nie dotyczy	Brak rekomendacji.
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	Brak podpisanej umowy powierzenia z podmiotem dostarczającym usługi hostingowe oraz z podmiotem serwisującym system typu SAP. W związku z powyższym brak możliwości zweryfikowania czy podmioty te wdrożyły odpowiednie zabezpieczenia techniczne i organizacyjne.	Stwierdzona niezgodność	Rekomenduje się przed zawarciem umowy powierzenia wysłanie do podmiotów przetwarzających ankiety bezpieczeństwa, której celem będzie weryfikacja zabezpieczeń technicznych i organizacyjnych.
Czy powierzenie przetwarzania danych osobowych odbywa się w granicach i na podstawie umowy lub instrumentu prawnego wymaganego przez RODO? Źródło: art. 28 ust. 3	Umowa powierzenia, o której mowa w art. 28 RODO nie została zawarta.	Stwierdzona niezgodność	Rekomenduje się zawarcie umowy powierzenia.

Czy podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego jedynie za uprzednią wiedzą i zgodą administratora? Źródło: art. 28 ust. 2	Nie została zawarta umowa powierzenia z podmiotami przetwarzającymi, w związku z powyższym audytowana organizacja nie posiada wiedzy czy dane są podpowierzane.	Potencjalna niezgodność	Rekomenduje się zawarcie umowy powierzenia i uregulowanie kwestii dalszego powierzenia danych.
Czy podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego na podstawie dokumentu prawidłowo określającego obowiązki stron? Źródło: art. 28 ust. 4	Audytowana organizacja nie posiada wiedzy w tym zakresie.	Potencjalna niezgodność	Rekomenduje się zawarcie umowy powierzenia.
WSPÓŁADMINISTROWANIE			
Czy współadministratorzy w przejrzysty sposób określili podział obowiązków wynikających z RODO? Źródło: art. 26 ust. 1 RODO	Dane nie są współadministrowane.	Nie dotyczy	Brak rekomendacji.
Czy osoba, której dane dotyczą, może korzystać z praw wynikających z RODO wobec każdego ze współadministratorów? Źródło: art. 26 ust. 3	Dane nie są współadministrowane.	Nie dotyczy	Brak rekomendacji.
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	Dane co do zasady nie są przekazywane do Państw trzecich. Z uwagi na brak umowy powierzenia z dostawcą usług hostingowych audytowana organizacja nie jest wstanie wykluczyć transferu.	Potencjalna niezgodność	Należy zweryfikować czy dostawca usług hostingowych nie transferuje danych do państwa trzeciego.

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	Dane nie są przekazywane do państwa trzeciego na podstawie art. 49 RODO.	Nie konsultowano ocenę skutków planowanych operacji przetwarzania dla ochrony danych osobowych z osobami, których dane dotyczą lub ich przedstawicielami.	Konsultowano ocenę skutków planowanych operacji przetwarzania dla ochrony danych osobowych z inspektorem ochrony danych.
OCENA KONIECZNOŚCI PRZEPROWADZENIA DPIA			
Pytanie i jego źródło w RODO	Odpowiedź (jak jest?)		Uzasadnienie
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		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.
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		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		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		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.

OBSZAR NR V
ANALIZA STOSOWANYCH PRZEZ ORGANIZACJA ORGANIZACYJNYCH I TECHNICZNYCH ŚRODKÓW OCHRONY DANYCH OSOBOWYCH

USTALENIA AUDYTOWE

Analiza spełnienia przez organizację nałożonych na nią w badanym obszarze obowiązków pozwoliła ustalić, co następuje

FIZYCZNA GRANICA OBSZARU PRZETWARZANIA DANYCH			
Pytanie i jego źródło w RODO	Odpowiedź (jak jest?)	Stopień zgodności	Rekomendacje (jak powinno być?)
Czy zapewniono, że budynek/budynki organizacji nie posiadają w swoich granicach punktów lub wad konstrukcyjnych, które mogłyby zostać wykorzystane do przedostania się do obszaru przetwarzania danych osobowych przez osoby nieupoważnione? Źródło: art. 32 ust. 1 RODO, ISO/IEC 27002, pkt 11.1.1 lit. b	Nie ujawniono wyraźnych luk ani punktów, poprzez które łatwo byłoby się włamać do obszaru przetwarzania danych organizacji. Zastrzeżenie budzi fakt możliwości niedomknięcia przez pracowników organizacji/dostawców w zewnętrznych nienadzorowanych przez recepcję drzwi wejściowych od strony szybu windy towarowej, co też miało miejsce w przeszłości. Wszystkie tego typu wejścia wyposażono w system kontroli dostępu oraz w samodomykacze drzwi. Dodatkowo w ramach zabezpieczeń przed dostępem fizycznym administrator budynku dostarczył system monitoringu wizyjnego.	Możliwość doskonalenia	W ramach doskonalenia zabezpieczeń fizycznego dostępu do obszaru przetwarzania danych osobowych organizacji zaleca instalację czujników domknięcia drzwi wejściowych. Ich zadaniem byłoby informowanie sygnałem dźwiękowym pracowników organizacji o ich nie domknięciu przez czas dłuższy niż np. 60 sekund.

Czy zapewniono dodatkowe zabezpieczenia budynku/budynków organizacji, uniemożliwiające przedostanie się do obszaru przetwarzania danych osobowych osobom nieupoważnionym? Źródło: art. 32 ust. 1 RODO, ISO/IEC 27002, pkt 11.1.1 lit. b.	Nie stwierdzono niezgodności. Nadzór nad bezpieczeństwem organizacji sprawuje całodobowa ochrona budynku. Dodatkowo dostęp dla gości do obszaru przetwarzania danych osobowych umożliwiony jest po uprzedniej rejestracji w głównej recepcji budynku oraz po przekazaniu karty dostępowej umożliwiającej przedostanie się przez bramki oraz windy na 10 piętro, na którym znajduje się organizacja. Przyznawana karta nie umożliwia dostępu przez jakiekolwiek inne drzwi w obszarze przetwarzania danych osobowych.	Zgodność	Brak rekomendacji.

Czy zapewniono zabezpieczanie okien i drzwi pomieszczeń organizacji, w których przetwarza się dane osobowe, na czas nieobecnosci osoby upoważnionej? Źródło: art. 32 ust. 1 RODO, ISO/IEC 27002, pkt 11.1.1 lit. b	Podczas wizji lokalnej ujawniono obecność nie zabezpieczonych drzwi pomieszczeń biurowych, w których zachodzi proces przetwarzania danych osobowych. Zidentyfikowane pomieszczenia pozostawione były na czas nieobecności osób upoważnionych. Pomieszczenia biurowe, w tym pomieszczenie przeznaczone do przechowywania dokumentów (archiwum) nie są zamykane również po godzinach pracy.	Stwierdzona niezgodność	Zaleca się zobowiązanie pracowników organizacji do zamykania drzwi pomieszczeń, w których zachodzi proces przetwarzania danych osobowych na czas nieobecności osób upoważnionych. Każdy z pracowników powinien być wyposażony w swój klucz do drzwi pomieszczenia, w którym realizuje swoje czynności służbowe, a jako ostatnia osoba opuszczająca pomieszczenie zobowiązana powinna być je odpowiednio zabezpieczyć. Ponadto zaleca się, aby drzwi pomieszczenia archiwum były odbezpieczane tylko na wypadek wyraźnej potrzeby, a dostęp do kluczy ograniczony był, podobnie jak w przypadku pomieszczenia serwerowni tylko i wyłącznie dla minimalnej i niezbędnej ilości osób. W ramach doskonalenia i podwyższenia skuteczności powyższego zaleca się wdrożenie systemu kontroli dostępu do wszystkich drzwi pomieszczeń biurowych, w szczególności do pomieszczenia archiwum.

Czy zapewniono kontrolę dostępu fizycznego, która umożliwia przedostanie się do obszaru przetwarzania danych osobowych tylko osobom upoważnionym? Źródło: art. 32 ust. 1 i 4 RODO, ISO/IEC 27002, pkt 11.1.1 lit. c	W organizacji zastosowano skuteczny system kontroli dostępu do obszaru przetwarzania danych osobowych za pośrednictwem indywidualnej dla każdego pracownika karty magnetycznej. Administrator w razie potrzeby jest w stanie określić kto i w jakich godzinach przebywał w organizacji. W razie zgubienia karty pracownik zobowiązany jest poinformować o tym osobę upoważnioną oraz stosuje się procedurę jej natychmiastowej blokady oraz wyrobienia duplikatu.	Potencjalna niezgodność	W ramach doskonalenia zastosowanego systemu kontroli dostępu zaleca się konfigurację godzin i dni, w których dostęp dla poszczególnych pracowników organizacji jest możliwy lub zablokowany. Podczas wdrożenia konfiguracji należy uwzględnić osoby, które na wypadek sytuacji wyjątkowych powinny posiadać fizyczny dostęp do biura całodobowo np. pracownicy działu IT.
Czy zapewniono system przeciwpożarowy, a jego działanie jest regularnie testowane? Źródło: art. 32 ust. 1 RODO, ISO/IEC 27002, pkt 11.1.1 lit. b i e	Ustalono, że w organizacji zapewniono system przeciwpożarowy. W jego skład wchodzą m.in. czujniki zadymienia, wolnostojące gaśnice proszkowe, hydranty oraz zraszacze wodne. Nie ujawniono gaśnic bez ważnego przeglądu technicznego. W pomieszczeniu serwerowni nie zidentyfikowano zbędnych, łatwopalnych przedmiotów. Przed wejściem zastosowano gaśnicę przeznaczoną do gaszenia urządzeń pod napięciem.	Zgodność	Brak rekomendacji
Czy zapewniono system wykrywania włamań, a jego działanie jest regularnie testowane? Źródło: art. 32 ust. 1 RODO, ISO/IEC 27002, pkt 11.1.1 lit. f	Nie zainstalowano systemu przeciwwłamaniowego. Nadzór nad bezpieczeństwem fizycznym obszaru przetwarzania danych osobowych sprawuje całodobowa ochrona budynku.	Możliwość doskonalenia	W ramach doskonalenia zaleca się instalację systemu przeciwwłamaniowego z czujnikami ruchu umieszczonymi w szczególności w okolicach wszystkich drzwi wejściowych do obszaru przetwarzania danych osobowych.

Czy w ramach zabezpieczeń sieciowych wdrożono systemy monitorujące służące do wykrywania i zapobiegania włamaniom? Źródło: art. 32 ust. 1 RODO, ISO/IEC 27002, pkt 13.1.2	Nie wdrożono systemów monitorujących służących do zapobiegania włamaniom.	Stwierdzona niezgodność	Należy wdrożyć systemy kontroli ruchu sieciowego w postaci IPS(Intrusion Prevention System) oraz IDS(Intrusion Detection System).
Czy w ramach zabezpieczeń sieciowych dokonano rozdzielenia sieci lokalnej na odrębne grupy sieciowe? Źródło: art. 32 ust. 1 RODO, ISO/IEC 27002, pkt 13.1.3	W organizacji zostały wykreowane VLAN'y. Podział sieci lokalnej nastąpił ze względu na funkcjonujące urządzenia, systemy oraz grupy użytkowników.	Zgodność	Brak.

Poniższa grafika obrazuje procentowy stopień spełnienia przez badaną organizację przyjętych kryteriów audytu: