DYREKTOR
Samorządowego Przedszkola
z Oddziałami Integracyjnymi Nr 1
im. Wandy Chotomskiej
w Kościanie
mgr Izabela Hoffmann

.....

ZATWIERDZAM

Dokumentacja ochrony danych osobowych RODO

2018-05-28

Spis treści

1. Wprowadzenie

Celem niniejszego dokumentu jest opisanie zasad ochrony danych osobowych oraz dostarczenie podstawowej wiedzy z zakresu ich przetwarzania.

W celu zwiększenia świadomości obowiązków i odpowiedzialności pracowników, a tym samym skuteczności ochrony przetwarzanych zasobów, w dokumencie opisano podstawy prawne przetwarzania danych osobowych oraz prawa i wolności osób, których dane dotyczą, aby lepiej zrozumieć związek danych osobowych z prawami osób.

Dokument szczegółowo opisuje podstawowe zasady organizacji pracy zawarte w opisanych środkach technicznych i organizacyjnych, a także w odniesieniu do danych przetwarzanych elektronicznie w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Wszelkie zestawienia uzupełniające treść dokumentu zebrano w postaci załączników. Do najważniejszych należy Rejestr czynności przetwarzania wraz z analizą ryzyk dla poszczególnych wpisów. Analiza ryzyka obejmuje potencjalne scenariusze naruszeń praw i wolności osób, w związku z ich danymi osobowymi oraz konieczne do zastosowania środki organizacyjne i techniczne zapewniające ich bezpieczeństwo.

2. Podstawy prawne

Poniżej opisano aktualne przepisy prawne w zakresie ochrony danych osobowych oraz wybrane, najważniejsze definicje i terminy.

1.1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679

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) jest podstawą prawną przetwarzania danych osobowych w Unii Europejskiej mającą zastosowanie od 25 maja 2018 roku.

Zgodnie z artykułem 24 oraz motywem 78 rozporządzenia parlamentu europejskiego i rady (UE) 2016/679 administrator wdraża wewnętrzne polityki i środki, „aby móc wykazać przestrzeganie niniejszego rozporządzenia" proporcjonalne do czynności przetwarzania. Jego obowiązkiem jest również, zgodnie z art. 30, ust. 3, prowadzenie Rejestru czynności przetwarzania w formie pisemnej (w tym elektronicznej) oraz dokumentacja wszelkich naruszeń ochrony danych osobowych, zgodnie z art. 33, ust. 5. Powyższe wskazania realizuje niniejsza dokumentacja.

1.2. Definicje

W dokumencie przyjmuje się następującą terminologię zgodną z Rozporządzeniem Parlamentu Europejskiego i Radu (UE) 2016/679 i ustawą ochronie danych osobowych :

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)

Dane osobowe (art. 4 pkt 1 RODO) – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Szczególne kategorie danych (art. 9 RODO) – oznaczają następujące kategorie danych: pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby.

Przetwarzanie (art. 4 pkt 2 RODO) – oznacza operację 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.

Zbiór danych (art. 4 pkt 6 RODO) – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

Administrator (art. 4 pkt 7 RODO) – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

Podmiot przetwarzający (art. 4 pkt 8 RODO) – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

Odbiorca (art. 4 pkt 9 RODO) – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę 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.

Zgoda osoby, której dane dotyczą (art. 4 pkt 11 RODO) – oznacza 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.

Naruszenie ochrony danych osobowych (art. 4 pkt 12 RODO) – 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.

Przedsiębiorca (art. 4 pkt 18 RODO) – oznacza osobę fizyczną lub prawną prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą.

Organ nadzorczy (art. 4 pkt 22 RODO) – oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51.

3. Przetwarzanie danych osobowych

Jakiekolwiek operacje na danych są zgodne z prawem, jeśli spełniony jest przynajmniej jeden z poniższych warunków:

1. osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
2. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
3. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
4. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub

innej osoby fizycznej;

5. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
6. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Przetwarzanie szczególnych kategorii danych jest zabronione, chyba że jest spełniony przynajmniej jeden z warunków:

1. osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1;
2. przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;
3. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
4. przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;
5. przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
6. przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
7. przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;
8. przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny

zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3;

9. przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;
10. przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

4. Prawa i wolności osób, których dane dotyczą

Ustawodawca europejski stwierdza w art. 1 ust. 2, że „niniejsze rozporządzenie chroni podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych". Administrator winien mieć na uwadze fakt, iż bierze odpowiedzialność również za takie przetwarzanie danych osobowych, które narusza prawa i wolności osób nie odnoszące się wprost do danych.

Aby administrator mógł realizować obowiązek wdrażania odpowiednich środków technicznych i organizacyjnych w związku z ryzykiem naruszenia praw lub wolności osób, których dane dotyczą, powinien znać prawa przysługujące osobom, których dane dotyczą oraz wynikające z tych praw konsekwencje.

Wśród praw i wolności osób wprost wymienionych w RODO należy wymienić zwłaszcza te, które są skatalogowane w rozdziale III „Prawa osoby, której dane dotyczą

4.1. Prawo do zwięzłej, przejrzystej i zrozumiałej informacji ze strony administratora

Osoba, której dane dotyczą ma prawo uzyskiwać od administratora wszelkie informacje dotyczące realizacji obowiązku informacyjnego (art. 13-14) oraz do komunikacji z administratorem w związku z realizacją swoich praw (art. 15-22 i 34)

Osoba może uzyskać informacje pisemnie, w tym elektronicznie, oraz ustnie, jeśli tego zażąda. Z kolei administrator jest zobowiązany udzielić żądanych informacji bezzwłocznie, a przynajmniej do miesiąca. Jeśli administrator nie podejmuje takich działań, to musi zakomunikować to osobie, która skierowała do niego żądanie w tych samych terminach. Udzielenie informacji jest bezpłatne, chyba że ma ustawiczny charakter. Wówczas administrator może pobrać opłatę, uwzględniając koszty administracyjne, albo odmówić podjęcia działań.

4.2. Prawo do bycia poinformowanym w przypadku zbierania danych od osoby, której dane dotyczą

Administrator jest zobowiązany na podstawie art.13.1 RODO podać osobie, od której zbiera dane osobowe następujące informacje:

- swoją tożsamość i dane kontaktowe oraz swojego przedstawiciela – jeśli ma to zastosowanie;
- dane kontaktowe inspektora ochrony danych – jeśli ma to zastosowanie;
- cel przetwarzania danych osobowych i podstawę prawną;
- jeśli podstawą przetwarzania jest prawnie uzasadniony interes, art. 6 ust. 1 lit. f) – treść tego interesu;
- informacje o odbiorcach lub kategoriach odbiorców – jeśli istnieją;
- informacje o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony oraz informacje o zabezpieczeniach w szczególnych przypadkach – jeśli zachodzi takie przekazanie;

oraz dla zachowania rzetelności i przejrzystości (art.13 ust. 2):

- okres przechowywania danych lub kryteria ustania tego okresu;
- informacje o prawach do: dostępu do danych osobowych osoby, której dane dotyczą, ich sprostowania, usunięcia i przenoszenia oraz o prawach do sprzeciwu wobec przetwarzania i ograniczeniu przetwarzania;
- informacje o prawie do cofnięcia zgody – jeśli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit a);
- informacje o prawie wniesienia skargi do organu nadzorczego;
- informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i określenia konsekwencji niepodania danych;
- informacje o zautomatyzowanym podejmowaniu decyzji i istotnych zasadach ich podejmowania, znaczeniu i przewidywanych konsekwencjach dla osoby, której dane

dotyczą.

Osoba ma prawo uzyskać informacje o celu i wypełnieniu obowiązków z ust. 2 jeśli administrator planuje przetwarzać zebrane już dane w innym celu.

Wzór obowiązku informacyjnego stanowi załącznik nr 7 do niniejszej dokumentacji.

4.3. Prawo do bycia poinformowanym w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą

Na podstawie art. 14 RODO Administrator jest zobowiązany podać osobie, której dane osobowe uzyskał z innych źródeł niż ta osoba następujące informacje (ust. 1):

- swoją tożsamość i dane kontaktowe oraz swojego przedstawiciela – jeśli ma to zastosowanie);
- dane kontaktowe inspektora ochrony danych – jeśli ma to zastosowanie;
- cel przetwarzania danych osobowych i podstawę prawną;
- kategorie przetwarzanych danych osobowych;
- informacje o odbiorcach lub kategoriach odbiorców – jeśli istnieją;
- informacje o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony oraz informacje os zabezpieczeniach w szczególnych przypadkach – jeśli zachodzi takie przekazanie;

oraz dla zachowania rzetelności i przejrzystości (ust. 2):

- okres przechowywania danych lub kryteria ustania tego okresu;
- prawnie uzasadniony interes administratora lub osób trzecich – jeśli podstawą przetwarzania jest art. 6 ust. 1 lit. f);
- informacje o prawach do: dostępu do danych osobowych osoby, której dane dotyczą, ich sprostowania, usunięcia i przenoszenia oraz o prawach do sprzeciwu wobec przetwarzania i ograniczeniu przetwarzania;
- informacje o prawie do cofnięcia zgody – jeśli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit a);
- informacje o prawie wniesienia skargi do organu nadzorczego;
- źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych;
- informacje o zautomatyzowanym podejmowaniu decyzji i istotnych zasadach ich podejmowania, znaczeniu i przewidywanych konsekwencjach dla osoby, której dane dotyczą.

Administrator jest zwolniony z realizacji powyższych obowiązków jeśli:

- osoba, której dane dotyczą posiada już takie informacje (np. administrator, który przekazał dane wypełnił już obowiązek informacyjny, także odnośnie celów i odbiorców);
- nie ma możliwości przekazać tych informacji lub wymagałoby to niewspółmiernie dużego wysiłku;
- pozyskiwanie lub ujawnianie danych jest wyraźnie uregulowane prawem Unii lub państwa członkowskiego oraz administrator przewiduje odpowiednie środki ochrony interesów osoby, której dane dotyczą;
- dane są poufne, co wynika z obowiązku zachowania tajemnicy zawodowej;
- uniemożliwi lub utrudni to prawidłowe wykonanie zadania publicznego, a interes lub prawa i wolności osoby, której dane dotyczą nie są nadrzędne w stosunku do interesu wynikającego z realizacji zadania publicznego (art. 5 ust. 1 pkt. 1);
- naruszy ochronę informacji niejawnych (art. 5 ust. 1 pkt. 2).

4.4. Prawo dostępu przysługujące osobie, której dane dotyczą

Na podstawiawie art. 15 RODO osoba, której dane dotyczą może, na żądanie, uzyskać od administratora potwierdzenie, że przetwarzane są dane osobowe jej dotyczące, a wówczas jej uprawniona do dostępu do nich oraz następujących informacji o:

- celach przetwarzania;
- kategoriach danych osobowych;
- odbiorcach lub kategoriach odbiorców, zwłaszcza z państw trzecich i organizacji międzynarodowych – jeśli ma to zastosowanie: o odpowiednich zabezpieczeniach;
- planowanym okresie przechowywania danych osobowych lub przynajmniej kryteria ustania tego okresu;
- prawach do: żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych tej osoby oraz o prawie do sprzeciwu wobec tego przetwarzania;
- prawie do wniesienia skargi do organu nadzorczego;
- źródłach pozyskania danych;
- tym, czy przetwarzanie będzie polegało również na zautomatyzowanym podejmowaniu decyzji.

Ponadto administrator dostarcza kopię przetwarzanych danych osobowych osobie, której dane dotyczą. Za kolejne kopie administrator może pobrać stosowną opłatę w związku z kosztami administracyjnymi.

Przepisu nie stosuje się, jeśli osoba, której dane dotyczą nie jest informowana na podstawie art. 5

ust. 1 ustawy, tj. uniemożliwia to prawidłowe wykonanie zadania publicznego przy jednoczesnej jego nadrzędności w stosunku do praw osób lub mogłoby to naruszyć ochronę informacji niejawnych.

4.5. Prawo do sprostowania danych

Na podstawie art. 16 RODO osobie, której dane dotyczą przysługuje prawo do żądania od administratora niezwłocznego sprostowania swoich danych, jeśli są nieprawidłowe. Ponadto, może zażądać również uzupełnienia niekompletnych danych, jeśli jest to zgodne z celem przetwarzania.

4.6. Prawo do usunięcia danych („prawo do bycia zapomnianym")

Na podstawie art. 17 RODO osoba, której dane dotyczą może zażądać od administratora usunięcia dotyczących jej danych osobowych, jeśli zachodzi jedna z podanych okoliczności:

- dane osobowe nie są już niezbędne do celów, w których były przetwarzane;
- osoba, której dane dotyczą cofnęła zgodę i nie ma innych podstaw do przetwarzania;
- osoba, której dane dotyczą sprzeciwiła się wobec przetwarzania i nie istnieje nadrzędna i prawnie uzasadniona podstawa przetwarzania lub osoba, której dane dotyczą sprzeciwia się marketingowi bezpośredniemu;
- dane osobowe były przetwarzane niezgodnie z prawem;
- administrator musi wywiązać się z obowiązku prawnego Unii bądź państwa członkowskiego, którym podlega;
- dane osobowe zostały zebrane w celu oferowania usług społeczeństwa informacyjnego od dziecka, które nie ukończyło 16 lat.

Administrator musi niezwłocznie wykonać to żądanie. Jeśli upublicznił te dane to, podejmując rozsądne działania i biorąc pod uwagę technologię i koszt realizacji, informuje administratorów przetwarzających te dane o żądaniu osoby. Administrator jest zwolniony z powyższych obowiązków, jeśli przetwarzanie jest niezbędne do:

- korzystania z prawa do wolności wypowiedzi;
- wywiązania się z obowiązku prawnego Unii bądź państwa członkowskiego, którym podlega lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej;
- zachowania interesu publicznego w dziedzinie zdrowia publicznego (np. zabezpieczenie społeczne, opieka zdrowotna);
- celów archiwalnych w interesie publicznym, badań naukowych, historycznych lub statystycznych, jeśli prawo to utrudnia realizację tych celów;
- ustalenia, dochodzenia lub obrony roszczeń.

4.7. Prawo do ograniczenia przetwarzania

Na podstawie art. 18 RODO osoba, której dane dotyczą może zażądać od administratora ograniczenia przetwarzania (tj. zaprzestania przetwarzania poza przechowywaniem), jeśli zachodzi jedna z podanych okoliczności:

- osoba ta kwestionuje prawidłowość przetwarzanych danych osobowych, a przetwarzanie ogranicza się na okres wyjaśnienia nieprawidłowości;
- przetwarzanie jest niezgodne z prawem, ale osoba, której dane dotyczą sprzeciwia się ich usunięciu, żądając w zamian ograniczenia przetwarzania;
- administrator nie potrzebuje danych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą do ustalenia, dochodzenia lub obrony roszczeń;
- osoba, której dane dotyczą wniosła sprzeciw wobec przetwarzania, wówczas przetwarzanie ogranicza się na czas stwierdzenia czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu.

Dane osobowe ograniczone tym prawem można przetwarzać tylko jeśli:

- osoba, której dane dotyczą wyraziła na to zgodę;
- do ustalenia, dochodzenia lub obrony roszczeń;
- w celu ochrony praw innej osoby fizycznej lub prawnej;
- z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego a osoba, której dane dotyczą zostanie o tym poinformowana.

4.8. Prawo do uzyskania powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania.

Na administratorze spoczywają dwa obowiązki w związku z realizacją tego prawa (art.19 RODO).

Po pierwsze, musi on powiadomić każdego odbiorcę, któremu ujawniono dane osobowe, jeśli te dane sprostował, usunął lub ograniczył. Administrator jest zwolniony z tego obowiązku, jeśli nie ma możliwości go wypełnić lub wymaga to niewspółmiernie dużego wysiłku.

Po drugie, osoba, której dane dotyczą ma prawo zażądać informacji o tych odbiorcach.

4.9. Prawo do przenoszenia danych.

Zgodnie z art. 20 ust. 1 RODO „osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono

te dane osobowe", jeśli:

- podstawą przetwarzania jest zgoda lub wykonanie umowy;
- oraz przetwarzanie odbywa się w sposób zautomatyzowany.

Osoba, której dane dotyczą może zażądać od administratora przesłania tych danych innemu administratorowi, jeśli jest to technicznie możliwe. Co ważne, prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

4.10. Prawo do sprzeciwu wobec przetwarzania.

Zgodnie z art. 21 ust. 1 RODO „Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych [...] w tym profilowania", jeśli podstawą tego przetwarzania jest:

- wykonanie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- prawnie uzasadniony interes realizowany administratora lub stronę trzecią.

Wówczas administrator nie może już przetwarzać danych, chyba że wykaże istnienie innych ważnych prawnie uzasadnionych podstaw przetwarzania nadrzędnych wobec interesów osoby, której dane dotyczą.

Jeśli dane są przetwarzane na potrzeby marketingu bezpośredniego (w tym profilowania), osoba, której dane dotyczą, może wnieść sprzeciw w dowolnym momencie. Wówczas administrator nie może już przetwarzać danych w tym celu.

4.11. Prawa w związku z zautomatyzowanym przetwarzaniem, w tym profilowaniem.

Na podstawie art. 22 RODO osoba, której dane dotyczą, ma prawo nie podlegać decyzjom opartym wyłącznie o zautomatyzowane przetwarzanie, w tym o profilowanie, jeśli wywołuje to wobec niej skutki prawne lub wpływa w inny istotny sposób. Prawo to nie przysługuje osobie, jeśli decyzja ta:

- jest niezbędna do zawarcia lub wykonania umowy między nią a administratorem;
- jest dozwolona prawem Unii lub prawem państwa członkowskiego, którym podlega administrator i przewiduje właściwe środki ochrony praw, wolności i interesów osoby;
- opera się na wyraźnej zgodzie osoby.

Osobie, której dane dotyczą, przysługują prawa do: ludzkiej interwencji ze strony administratora, wyrażenia własnego stanowiska i zakwestionowania decyzji; jeśli podstawą decyzji jest zawarcie lub wykonanie umowy albo zgoda.

Osoba, której dane dotyczą, ma prawo by decyzje te nie opierały się na szczególnych kategoriach danych osobowych, poza przypadkami kiedy:

- wyraża na to zgodę;
- przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

4.12. Prawo do wyrażania zgody I jej wycofania.

Art. 4 ust. 11 definiuje czym jest zgoda – „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".

Na administratorze spoczywa obowiązek wykazania, że zgoda została uzyskana prawidłowo (art.7 ust. 1). Ponadto, zgoda musi być wyodrębniona spośród innych zagadnień, jeśli jest wyrażana na piśmie, a także być sformułowana prostym i zrozumiałym językiem (art. 7 ust. 2).

Administrator musi także poinformować osobę, której dane dotyczą o prawie do wycofania zgody w dowolnym momencie jeszcze przed jej wyrażeniem. Jeśli część oświadczenia jest niezgodna z RODO, wówczas zgoda jest nieważna; podobnie, gdy od jej wyrażenia jest uwarunkowane wykonanie umowy (art. 7 ust. 4).

Wyrażenie zgody przez dziecko w przypadku usług społeczeństwa informatycznego (np. portale społecznościowe) wymaga ponadto, aby zgodę wyraził lub zaaprobował rodzic lub prawny opiekun (art. 8). Dotyczy to dzieci do lat 16 (państwo członkowskie może obniżyć ten wiek do 13 lat; polski ustawodawca nie zdecydował się na takie rozwiązanie).

Wyraźna zgoda jest też jednym z możliwych warunków przetwarzania szczególnych kategorii danych osobowych (art. 9 ust. 2 lit. a).

4.13. Prawo do bycia poinformowanym o naruszeniu ochrony danych osoby, której dane dotyczą.

Na podstawie art. 34 RODO osoba, której dane dotyczą ma prawo uzyskać informacje o naruszeniu ochrony jej danych, jeśli to naruszenie może powodować wysokie ryzyko naruszenia innych jej praw lub wolności.

Taka informacja musi prosto i jasno opisywać charakter naruszenia, wskazać dane kontaktowe Inspektora ochrony danych, opisywać możliwe konsekwencje oraz zastosowane środki ochrony.

Administrator nie musi realizować tego prawa w czterech przypadkach:

- wdrożył odpowiednie środki techniczne i organizacyjne ochrony, w szczególności szyfrowanie, lub
- wdrożył środki eliminujące wysokie ryzyko, lub
- wymagałoby to niewspółmiernie dużego wysiłku, lub

organ nadzorczy orzekł, że został spełniony, któryś z wcześniejszych warunków.

4.14. Na podstawie art. 38.4 RODO osoba, której dane dotyczą może kontaktować się z właściwym Inspektorem administratora, podmiotu przetwarzającego lub ich przedstawicieli w celu.

- uzyskania informacji o przetwarzaniu swoich danych lub
- uzyskania informacji o prawach przysługujących jej na mocy RODO.

4.15. Prawo do wniesienia skargi do organu nadzorczego.

Na podstawie art. 77 RODO - „Każda osoba, której dane dotyczą, ma prawo wnieść skargę do organu nadzorczego, [...] jeżeli sądzi, że przetwarzanie danych osobowych jej dotyczące narusza niniejsze rozporządzenie."

4.16. Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko organowi nadzorczemu.

Na podstawie art. 78 RODO - „Każda osoba fizyczna lub prawna ma prawo do skutecznego środka ochrony prawnej przed sądem przeciwko prawnie wiążącej decyzji organu nadzorczego jej dotyczącej."

4.17. Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu.

Na podstawie art. 79 RODO - „Każda osoba, której dane dotyczą, ma prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli uzna ona, że prawa przysługujące jej na mocy niniejszego rozporządzenia zostały naruszone w wyniku przetwarzania [jej] danych osobowych z naruszeniem niniejszego rozporządzenia."

4.18. Prawo do odszkodowania.

Na podstawie art. 82 ust.1 RODO - „Każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę."

Administrator odpowiada za szkody spowodowane przetwarzaniem naruszającym przepisy rozporządzenia, zaś podmiot przetwarzający odpowiada w zakresie niedopełnienia obowiązków wynikających z rozporządzenia lub działania poza lub wbrew instrukcjom administratora.

5. Podstawowe obowiązki Administratora danych osobowych

Obowiązki administratora danych osobowych zostały ściśle określone w rozdziale IV RODO.

W ramach sekcji 1. ustawodawca europejski wymienia ogólne obowiązki przede wszystkim administratorów, mówiąc również o zadaniach współadministratorów i podmiotów przetwarzających.

Sekcje 2., 3., 4. i 5. dotyczą kolejno bezpieczeństwa danych osobowych, oceny skutków dla ochrony danych, inspektora ochrony danych i kodeksów postępowania oraz certyfikacji. Poszczególne elementy tych sekcji zawarte są w innych paragrafach.

5.1. Wdrażanie odpowiednich środków technicznych I organizacyjnych.

Na administratorze spoczywa obowiązek wdrażania odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z RODO. Wdrażanie jest czynnością permanentną i należy przez nie rozumieć również utrzymywanie i przegląd używanych środków. Wynika to ze stale zmieniających się okoliczności przetwarzania, na które składa się: charakter przetwarzania, zakres, kontekst i cele oraz ryzyko naruszenia praw lub wolności osób fizycznych.

Uwagę należy zwrócić zwłaszcza na ryzyko naruszenia praw i wolności osób o różnym prawdopodobieństwie i wadze zagrożenia. Wskazane jest, aby administrator wykonał szacowanie i ocenę ryzyka czynności przetwarzania, aby sprostać wymogom RODO, co do ochrony w fazie

projektowania, domyślnej ochrony, bezpieczeństwa przetwarzania oraz oceny skutków. Wynikiem tego procesu mają być indywidualne wskazania dla organizacji, jak należy chronić daną czynność (proces) przetwarzania.

Konieczne do stosowania środki techniczne i organizacyjne zostały określone indywidualnie dla każdej czynności przetwarzania po przeprowadzeniu dla niej analizy ryzyka, stąd zawarte zostały w załącznikach nr 1 oraz nr 2 do niniejszej dokumentacji oraz w Instrukcji zarządzania systemem informatycznym będącej załącznikiem nr 8 do niniejszej dokumentacji.

Zestawienie zalecanych środków technicznych I organizacyjnych:

- Przetwarzanie danych osobowych może odbywać się wyłącznie w ramach wykonywania zadań służbowych. Zakres uprawnień wynika z zakresu tych zadań.
- Prowadzona jest ewidencja osób upoważnionychdo przetwarzania danych.
- Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne upoważnienie. Podpisany dokument jest dołączany do akt osobowych.
- Każdy pracownik odbywa szkolenie z zakresu ochrony danych osobowych. Szkolenie może być wewnętrzne, tj. samokształcenie na podstawie materiałów przygotowanych przez Inspektora ochrony danych, bezpośrednio prowadzone przez Inspektora ochrony danych lub zewnętrzne, prowadzone przez firmy specjalistyczne. Nowo przyjęty pracownik odbywa szkolenie przed przystąpieniem do przetwarzania danych.
- Ponadto każdy upoważniony do przetwarzania danych potwierdza pisemnie, na dokumencie upoważnienia, fakt zapoznania się z niniejszą dokumentacją i zrozumieniem wszystkich zasad bezpieczeństwa. Podpisany dokument jest dołączany do akt osobowych.
- Obszar przetwarzania danych osobowych zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.
- Przebywanie osób, nieuprawnionych w w/w obszarze jest dopuszczalne za zgodą Administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
- Pomieszczenia stanowiące obszar przetwarzania danych powinny być zamykane na klucz.
- Przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna oraz usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w odpowiednich zamykanych szafach lub biurkach.
- Nie należy dopuszczać osób nie mających uprawnień do danych osobowych do treści tych danych, np. pokazywanie dokumentów.
- Dokumenty zawierające dane osobowe należy niszczyć w specjalistycznych niszczarkach.
- Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w

sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.

- Dokumenty w wersji elektronicznej, które zapisywane są na nośniki zewnętrzne, przenoszone poza obszar przetwarzania lub przesyłane pocztą elektroniczną, należy zabezpieczyć poprzez nadanie im haseł odczytu.
- Zbiory osobowe przetwarzane elektronicznie należy zabezpieczać poprzez wykonywanie kopii bezpieczeństwa, zapisywanych na zewnętrznych nośnikach i przechowywanych pod zamknięciem.
- Komputery, które przetwarzają dane osobowe należy wyposażyć w urządzenia podtrzymujące napięcie na wypadek braku zasilania.
- W celu zapewnienia danych przetwarzanych elektronicznie należy zapewnić logowanie do systemu operacyjnego oraz bezpośrednio do programów przetwarzających dane.
- Szczegółowe zasady postępowania z danymi osobowymi przetwarzanymi elektronicznie określa Instrukcja zarządzania systemem informatycznym będąca częścią niniejszej dokumentacji.
- Administrator danych stwierdzając w ramch nadzoru, konieczność utworzenia w problemowm obszarze bezpieczeństwa szczegółowej instrukcji postepowania, wdraża jej postanowienia odrębnym dokumentem wewnętrznym.

5.2. Uwzględnianie ochrony danych osobowych w fazie projektowania oraz domyślna ochrona danych.

Zgodnie z zasadami dotyczącymi przetwarzania danych osobowych (art. 5 RODO), administrator już w fazie projektowania, a dalej w trakcie przetwarzania, uwzględnia odpowiednie środki techniczne i organizacyjne ochrony. RODO wymienia niektóre sposoby, takie jak pseudonimizacja czy minimalizacja danych. Zawsze właściwym narzędziem do wdrażania tych i podobnych środków jest szacowanie i ocena ryzyka, aby środki te były adekwatne do kontekstu organizacji.

5.3. Rejestrowanie czynności przetwarzania.

Administrator jest zobowiązany na podstawie art. 30 RODO do prowadzenia rejestru czynności przetwarzania. Minimalny zakres informacji, które należy zawrzeć we wpisie w rejestrze, wymienia ust. 1:

- imię i nazwisko lub nazwa oraz dane kontaktowe administratora, wszelkich współadministratorów, a gdy ma to zastosowanie również przedstawiciela administratora i inspektora ochrony danych – przynajmniej w nagłówku rejestru;
- cele przetwarzania;
- opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych;
- kategorie odbiorców danych osobowych, w tym odbiorców w państwach trzecich i organizacjach międzynarodowych;

- przekazanie danych do państwa trzeciego lub organizacji międzynarodowej, a w szczególnych przypadkach dokumentacja tych zabezpieczeń, gdy następuje takie przekazanie;
- w miarę możliwości, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

W rejestrze można umieszczać także inne, stosowne informacje, na przykład: podstawę prawną, źródło pochodzenia danych i inne.

Z kolei podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania. Minimalny zakres informacji, które należy zawrzeć we wpisie w rejestrze, wymienia ust. 2

- imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego i podmiotów przetwarzających oraz każdego administratora, w imieniu którego przetwarza dane, a gdy ma to zastosowanie również przedstawiciela podmiotu przetwarzającego i inspektora ochrony danych – przynajmniej w nagłówku rejestru;
- kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
- przekazanie danych do państwa trzeciego lub organizacji międzynarodowej, a w szczególnych przypadkach dokumentacja tych zabezpieczeń; gdy następuje takie przekazanie;
- w miarę możliwości, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

Podmiot przetwarzający, analogicznie do rejestru czynności przetwarzania, może zawrzeć również inne informacje w ramach rejestru kategorii czynności przetwarzania.

Należy zwrócić uwagę, że organizacja może jednocześnie pełnić rolę administratora i podmiotu przetwarzającego i w związku z tym, realizując jedne czynności przetwarzania, będzie zobligowana do wciągnięcia ich w rejestr czynności przetwarzania, zaś realizując czynności powierzone, będzie podlegać obowiązkowi prowadzenia rejestru kategorii czynności przetwarzania. Rejestry te prowadzone są oddzielnie.

Rejestry te mają być udostępniane na żądnie organu nadzorczego.

Zwolnieniu z obowiązku prowadzenia tych rejestrów podlega przedsiębiorca zatrudniający mniej niż 250 osób, chyba że jego przetwarzanie może powodować wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa. Nie można wykluczyć tych okoliczności bez uprzedniego przeanalizowania czynności przetwarzania czemu również służy szacowanie i ocena ryzyka.

Rejestr czynności przetwarzania wraz z analizą ryzyka określającą konieczne do stosowania środki techniczne i organizacyjne stanowią załączniki nr 1 i nr 2 do niniejszej dokumentacji.

Jeżeli ma to zastosowanie, rejestr kategorii czynności przetwarzania stanowi załącznik nr 15 do niniejszej dokumentacji.

5.4. Współpraca z organem nadzorczym.

Zarówno administrator, jak i podmiot przetwarzający, a także Inspektor ochrony danych na żądanie organu nadzorczego współpracują z nim w zakresie zadań wykonywanych przez ten organ.

6. Dokumentowanie

RODO nie zawiera wprost wyrażonego obowiązku prowadzenia dokumentacji ochrony danych osobowych. Jednakże na podstawie kilku przesłanek należy stwierdzić, iż prowadzenie dokumentacji jest konieczne, aby sprostać wymaganiom rozporządzenia. Te przesłanki to:

- Zasada rozliczalności (art. 5 ust. 2 RODO): Administrator odpowiada za przestrzeganie zasad przetwarzania danych osobowych oraz musi być w stanie wykazać ich przestrzeganie.
- Rejestr czynności przetwarzania oraz rejestr kategorii czynności przetwarzania mają formę pisemną, w tym elektroniczną (art. 30 ust. 3 RODO)
- Administrator ma obowiązek dokumentować wszelkie okoliczności naruszenia ochrony danych (art. 33 ust. 5 RODO).

Aby sprostać tym i innym wymaganiom RODO, wskazane jest, aby prowadzić dokumentację w formie pisemnej, w tym elektronicznej, która zawiera przynajmniej:

- rejestr czynności przetwarzania lub rejestr kategorii czynności przetwarzania, w zależności od tego, co ma zastosowanie;
- rejestr naruszeń;
- ewidencję osób upoważnionych;
- zasady pracy w systemie informatycznym.

Ponadto integralnym elementem takiej dokumentacji jest proces szacowania i oceny ryzyka każdej czynności przetwarzania, który zawiera takie informacje jak: wykorzystywane aktywa, zagrożenia, podatności, istniejące i planowane zabezpieczenia. Z niego wynikają poszczególne zalecenia dla organizacji, takie jak środki techniczne i organizacyjne, które należy wdrożyć i stosować.

7. Upoważnienie do przetwarzaia danych

W odniesieniu do art. 29 i 32 ust. 4 RODO administrator lub podmiot przetwarzający upoważnia osobę lub podmiot przetwarzający do dostępu do danych i ich przetwarzania wyłącznie w wyznaczonym przez siebie zakresie, chyba że prawo Unii lub państwa członkowskiego wymaga tego od tej osoby lub podmiotu.

Ponadto administrator i podmiot przetwarzający muszą podjąć takie działania, aby zapewnić, że upoważnieni działają tylko w wyznaczonym zakresie.

Ewidencję osób upoważnionych do przetwarzania danych stanowi załącznik nr 4 do niniejszej dokumentacji.

Wzór upoważnienia do przetwarzania danych osobowych z jednoczesnym oświadczeniem o znajomości zasad bezpieczeństwa, stanowi załącznik nr 5 do niniejszej dokumentacji.

8. System zarządzania ryzykiem

W odniesieniu do art. 24 i 32 prowadzi się system zarządzania ryzykiem. Elementami systemu są ewidencje aktywów, zagrożeń, podatności, skutków, zabezpieczeń i wyjątków akceptacji ryzyka oraz opis ryzyka czynności przetwarzania według Normy PN-ISO/IEC 27005:2014-01 „Technika informatyczna – Technika bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji" oraz zaleceń Generalnego Inspektora Ochrony Danych Osobowych.

W załącznikach nr 9 - 14 do niniejszej dokumentacji zestawiono, na podstawie danych z audytu przetwarzania danych osobowych, sumarycznie dla wszystkich czynności przetwarzania, ewidencje: aktywów, zagrożeń, podatności, zabezpieczeń, skutków oraz wyjątków akceptacji ryzyka.

Następnie, dane posłużyły do analiz ryzyk przeprowadzonych indywidualnie w stosunku do każdej czynności przetwarzania zarejestrowanej w Rejestrze czynności.

Końcowy efekt analizy ryzyka stanowi element załączników nr 1 oraz 2 do niniejszej dokumentacji.

9. Naruszenie ochrony danych osobowych.

Zgodnie z art. 4 pkt 12) RODO naruszenie ochrony danych 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."

Przykład naruszenia stanowią:

- przypadkowe lub umyślne usunięcie danych przez osobę nieupoważnioną;
- utrata hasła dostępu do danych osobowych;
- utrata dokumentów lub niezabezpieczonego nośnika danych z danymi osobowymi;
- kradzież danych osobowych przez zabranie dokumentów lub włamanie do sieci;
- przypadkowe przesłanie danych osobowych do osoby trzeciej.

Gdy dojdzie do naruszenia, administrator musi zastosować odpowiednie procedury:

- powiadomić Inspektora ochrony danych (jeśli go wyznaczył);
- ocenić, czy naruszenie może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych;
- przygotować zgłoszenie do organu nadzorczego – gdy jest ono wymagane;
- powiadomić osoby, których dane dotyczą o naruszeniu – gdy jest to wymagane;
- udokumentować wszelkie naruszenia w rejestrze naruszeń.

Wobec podmiotu przetwarzającego stosuje się tylko jeden wymóg, aby bez zbędnej zwłoki poinformował on administratora o naruszeniu (art. 33 ust. 2 RODO).

Administrator w pierwszym kroku powinien stwierdzić, jak wysokie jest prawdopodobieństwo naruszenia praw i wolności osób fizycznych w związku z naruszeniem. Jeśli to prawdopodobieństwo jest małe, wówczas takie naruszenie nie podlega zgłoszeniu do organu nadzorczego. W przypadkach kiedy prawdopodobieństwo jest średnie lub wysokie, należy zgłosić naruszenie do organu nadzorczego. Co ważne, termin zgłoszenia to 72 godziny od momentu stwierdzenia naruszenia. Zgłoszenie po wskazanym terminie musi być uzupełnione wyjaśnieniem przyczyn opóźnienia. Do określenia wartości prawdopodobieństwa można posłużyć się scenariuszami zdarzeń dla czynności przetwarzania, która została naruszona.

Zgłoszenie do organu nadzorczego, zgodnie z art. 33 ust.3, powinno zawierać co najmniej:

- opis charakteru naruszenia;
- w miarę możliwości kategorie i przybliżoną liczbę osób, których dane dotyczą;
- w miarę możliwości kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
- imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu informacyjnego;
- opis możliwych konsekwencji naruszenia;
- opis zastosowanych lub proponowanych przez administratora środków zaradczych, w tym środki służące w celu zminimalizowania ewentualnych negatywnych skutków.

W ten sam sposób można udokumentować w rejestrze naruszeń naruszenia, które nie podlegają zgłoszeniu do organu nadzorczego.

Gdy naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób, administrator bez zbędnej zwłoki zawiadamia osoby, których dane dotyczą. Aby stwierdzić, czy takie ryzyko istnieje, może posłużyć się wynikami scenariuszy zdarzeń dla czynności przetwarzania, która została naruszona. W art. 34 ust. 2 wskazano wymogi, jakie musi spełniać to zawiadomienie:

- napisane jasnym i prostym językiem;
- opisuje charakter naruszenia;
- zawiera imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu informacyjnego;
- opisuje możliwe konsekwencje naruszenia;
- opisuje zastosowanych lub proponowanych przez administratora środków zaradczych, w tym środki służące w celu zminimalizowania ewentualnych negatywnych skutków.

Administrator może być zwolniony z obowiązku informowania osób, których dane dotyczą o naruszeniu, jeśli wystąpi którykolwiek z przypadków z art. 34 ust. 3 i 4:

- administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie (szczególnie szyfrowanie);
- po naruszeniu, administrator zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
- wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób;
- Organ nadzorczy stwierdził, że spełniony został jeden z wcześniejszych warunków.

Rejestr naruszeń stanowi załącznik nr 3 do niniejszej dokumentacji.

10. Powierzenie przetwarzania danych

Na podstawie art. 28 Administrator może powierzyć przetwarzanie danych osobowych (lub część operacji tego przetwarzania) na podstawie umowy lub innego instrumentu prawnego podmiotowi przetwarzającemu.

Podmiot przetwarzający musi zapewnić „wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą" (art. 28 ust. 1). Podmiot przetwarzający może podpowierzyć przetwarzanie danych innemu podmiotowi, jednak tylko za uprzednią szczegółową lub ogólną pisemną zgodą administratora (art. 28 ust. 2) i pod warunkiem wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odbywało się zgodnie z rozporządzeniem (art. 28 ust. 4).

art. 28 ust. 3 reguluje elementy umów powierzenia oraz obowiązki podmiotu przetwarzającego. Elementy jakie należy zawrzeć w umowie powierzenia to:

- przedmiot i czas trwania przetwarzania;
- charakter i cel przetwarzania;
- kategorie danych osobowych i kategorie osób, których dane dotyczą;
- obowiązki i prawa administratora.

Umowa powierzenia może opierać się na standardowych klauzulach umownych (określonych przez Europejską Radę Ochrony Danych lub UODO) i ma formę pisemną, w tym elektroniczną.

Podmiot przetwarzający jest zobowiązany do:

- przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora, tj. zgodnie z jego instrukcjami, poza przypadkiem, kiedy jest zobowiązany do przetwarzania przepisem unijnym lub państwa członkowskiego, któremu podlega a wówczas informuje o tym administratora, chyba że to prawo zabrania udzielić takiej informacji z uwagi na ważny interes publiczny;
- zapewnienia, by osoby upoważnione do przetwarzania danych osobowych zachowywały tajemnicę;
- wdrażania środków technicznych i organizacyjnych, by zapewnić stopień ochrony adekwatny do ryzyka przetwarzania;
- przestrzegania zasad podpowierzenia (art. 28 ust. 2 i 4);

- pomagania administratorowi – w miarę możliwości – poprzez środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osób, w związku z realizacją ich praw i wolności określonych w rozdziale III, uwzględniając charakter przetwarzania;
- pomaga administratorowi wywiązać się z obowiązków zabezpieczania danych, zgłaszania naruszeń organowi nadzorczemu i osobom, których dane dotyczą i przeprowadzenia oceny skutków dla ochrony danych wraz z uprzednimi konsultacjami;
- usuwa lub zwraca administratorowi dane po zakończeniu świadczenia usług, chyba że inaczej nakazuje prawo Unii lub państwa członkowskiego, któremu podlega;
- udostępnienia administratorowi wszelkich informacji niezbędnych do wykazania spełnienia swoich obowiązków;
- umożliwienia administratorowi lub upoważnionemu przez niego audytorowi przeprowadzenie audytu, w tym inspekcji i przyczynia się do nich.

Jeśli podmiot przetwarzający narusza RODO przy określaniu celów i sposobów przetwarzania, to wówczas uznaje się go za administratora, jednak bez uszczerbku dla stosowania sankcji z art. 82-84.

Wzór umowy powierzenia stanowi załącznik nr 6 do niniejszej dokumentacji.

11. Wyznaczenie, status i zadania inspektora ochrony danych

Sposób wyznaczenia inspektora ochrony danych osobowych (dalej „IOD") reguluje art. 37 RODO. Administrator i podmiot przetwarzający wyznaczają IOD, gdy: są organem lub podmiotem publicznym albo ich główną działalnością jest regularne i systematyczne monitorowanie osób na dużą skalę, albo ich główną działalnością jest przetwarzanie szczególnych kategorii danych osobowych lub dotyczących wyroków skazujących.

Jeden IOD może być wyznaczony dla kilku podmiotów publicznych jednocześnie. IOD jest wyznaczony na podstawie kwalifikacji zawodowych, a szczególnie wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych osobowych oraz umiejętności wypełnienia zadań. IOD może być członkiem personelu administratora lub podmiotu przetwarzającego lub może wykonywać zadanie na podstawie umowy o świadczeniu usług.

Obowiązkiem administratora lub podmiotu przetwarzającego jest opublikowanie danych kontaktowych IOD i zawiadomienie o nich organ nadzorczy.

Status IOD reguluje art. 38 RODO. Zgodnie z nim administrator oraz podmiot przetwarzający:

- zapewniają, by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych (ust. 1),
- zapewniają mu zasoby do wykonania jego zadań, do utrzymania wiedzy fachowej oraz dostęp do danych osobowych i operacji przetwarzania (ust. 2),
- zapewniają by IOD nie otrzymywał od nich instrukcji dotyczących wykonywania swoich zadań i nie odwołują go ani karzą za wypełnianie swoich zadań (ust. 3),

a IOD:

- podlega bezpośrednio najwyższemu kierownictwu administratora lub podmiotu przetwarzającego (ust. 3);
- pełni rolę punktu kontaktowego dla osób, których dane dotyczą w związku z przetwarzaniem ich danych oraz praw przysługujących im na mocy RODO (ust. 4);
- zachowuje tajemnicę/poufność co do wykonywania swoich zadań – zgodnie z prawem Unii lub państwa członkowskiego (art. 5);
- może wykonywać inne zadania i obowiązki, jeśli administrator lub podmiot przetwarzający zapewnią, że nie spowoduje to konfliktu interesów, np. prowadzić dokumentację przetwarzania danych;

Zadania IOD zostały określone w art. 39. Do zadań IOD należy:

- informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
- monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;
- współpraca z organem nadzorczym;
- pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;

12. Przekazywanie danych do państwa trzeciego

Kwestię przekazywania danych do państw trzecich lub organizacji międzynarodowych reguluje rozdział V RODO. Poniżej zawarto najważniejsze wskazania odnośnie przekazywania danych:

- Przekazywanie danych osobowych do państw trzecich i organizacji międzynarodowych należy odnotować w rejestrze czynności przetwarzania i rejestrze kategorii czynności przetwarzania (art. 30 RODO).
- Przekazanie nie wymaga specjalnego zezwolenia Komisji, jeśli ta stwierdziła wcześniej, że państwo trzecie, terytorium czy organizacja międzynarodowa zapewnia odpowiedni stopień ochrony (takim państwem jest np. Szwajcaria).
- Przekazanie bez zezwolenia jest możliwe, jeśli administrator lub podmiot przetwarzający zapewnią odpowiednie zabezpieczenia (wymienione w art. 46 ust. 2 RODO), a prawa osób i środki ochrony prawnej obowiązują i są egzekwowalne.
- Dopuszczalne jest przekazanie bez odpowiednich zabezpieczeń, ale tylko, gdy zostaną spełnione warunki z art. 49 ust. 1 RODO.

13. Sankcje karne

Art. 83 RODO określa wysokość oraz kryteria nałożenia administracyjnej kary pieniężnej za naruszenia rozporządzenia. Ustawodawca europejski przyjmuje dwa progi maksymalne:

- 10 mln euro lub 2% rocznego światowego obrotu (zastosowanie ma kwota wyższa) za naruszenie: obowiązków administratora lub podmiotu przetwarzającego, podmiotu certyfikującego, podmiotu monitorującego;
- 20 mln euro lub 4% rocznego światowego obrotu (zastosowanie ma kwota wyższa) za naruszenie: zasad przetwarzania (w tym warunków zgody); praw osób, których dane dotyczą; przekazywania danych do państw trzecich i organizacji międzynarodowych; nakazów organu nadzorczego i inne.

Polski ustawodawca proponuje maksymalny próg dla jednostek sektora finansów publicznych w wysokości 100 tys. złotych poza państwowymi i samorządowymi instytucjami kultury, dla których proponuje kwotę w wysokości 10 tys. złotych.

Kryteria jakimi będzie posługiwał się organ nadzorczy są następujące:

- charakter, waga i czas trwania naruszenia z uwzględnieniem charakteru, zakresu i celu przetwarzania;
- umyślność;
- przeciwdziałanie szkodom poniesionym przez osoby, których dane dotyczą;
- stopień odpowiedzialności z uwzględnieniem wdrożonych środków technicznych i organizacyjnych;
- wcześniejsze naruszenia;

- stopień współpracy z organem nadzorczym;
- kategorie danych osobowych, których dotyczyło naruszenie;
- sposób, w jaki organ nadzorczy dowiedział się o naruszeniu oraz sposób zgłoszenia;

Państwa członkowskie mogą przyjąć przepisy określające także inne sankcje, w szczególności za naruszenia niepodlegające administracyjnym karom pieniężnym. Polski ustawodawca proponuje grzywnę, karę ograniczenia wolności albo pozbawienia wolności do lat dwóch za przetwarzanie danych, których przetwarzanie jest niedopuszczalne lub przetwarzanie bez uprawnienia oraz za udaremnianie i utrudnianie kontroli przestrzegania przepisów. Zwiększa karę pozbawienia wolności do lat trzech za ujawnienie szczególnych kategorii danych bez uprawnienia do ich przetwarzania lub gdy jest to niedopuszczalne.

14. Załącznik nr 1- rejestr czynności przetwarzania

ID	Nazwa czynności	Cel przetwarzania	Kategorie osób
1			
2			
3			
4			

1. Szczegóły czynności przetwarzania

Przetwarzanie	
Nazwa czynności:	
Nazwa i dane kontaktowe administratora:	
Nazwa i dane kontaktowe inspektora ochrony danych:	
Cel przetwarzania:	
Prawo	
Podstawa prawna:	
Dane	
Kategorie osób, których dane dotyczą:	
Kategorie danych osobowych:	
Szczególne kategorie:	
Planowany termin usunięcia:	
Uwagi do usunięcia:	
Odbiorcy	
Odbiorcy danych w państwach Unii Europejskiej:	
Odbiorcy danych w państwach trzecich:	
Przekazywanie	
Nazwa państwa trzeciego lub organizacji	
Dokumentacja odpowiednich zabezpieczeń w szczególnych wypadkach:	
Współpraca	
Współadministratorzy:	
Podmioty przetwarzające:	
Zabezpieczenia	
Środki techniczne i organizacyjne:	
Uwagi	
Uwagi:	

15. Załącznik nr 2 analiza ryzyka

Analiza ryzyka określająca stosowane oraz konieczne do stosowania środki techniczne i organizacyjne.

l	Nazwa czynności	Cel przetwarzania	Kategorie osób
1			
2			
3			
4			

18. Upoważnienie

....., dnia: .....

Sygnatura: .....

Ważność od: .....
Ważność do: .....

UPOWAŻNIENIE

Na podstawie art. 32.4 Rozporządzenia Parlamentu Europejskiego i Rady (UE) z dnia 27.04.2016 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, upoważniam Panią/Pana:

.....

do przetwarzania danych osobowych, niezbędnych do realizacji zadań służbowych, zgodnie z zakresem czynności określonym przez Administratora danych.

Niniejsze upoważnienie jest ważne do chwili jego odwołania lub rozwiązania/wygaśnięcia umowy o pracę.

Osoba upoważniona do przetwarzania danych osobowych objętych zakresem powyższego upoważnienia stwierdza własnoręcznym podpisem, że znana jest jej treść:

- dokumentacji ochrony danych osobowych,
- Rozporządzenia Parlamentu Europejskiego i Rady (UE) z dnia 27.04.2016 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

i zobowiązuje się do:

- Stosowania określonych przez Administratora danych środków technicznych I organizacyjnych określonych w dokumentacji
- stosowania zasad, procedur oraz wytycznych mających na celu właściwe i adekwatne w stosunku do celu przetwarzanie danych,
- należytego zabezpieczenia danych osobowych przed ich udostępnieniem osobom nie upoważnionym,
- zachowania szczególnej staranności w trakcie dokonywania operacji przetwarzania danych w celu ochrony osób, których dane dotyczą.

.....
podpis oświadczającego

.....
podpis Administratora danych

17. Załącznik nr 4 – ewidencja osób upoważnionych do przetwarzania danych

Lp.	Nazwisko i imię	Wydano/sygn	Ważność od	Ważność do	Czynność	Uwagi
1		2018-05-28 1/2018			Zgodnie z zakresem określonym przez administratora danych.	
2		2018-05-28 2/2018			Zgodnie z zakresem określonym przez administratora danych.	
3		2018-05-28 3/2018			Zgodnie z zakresem określonym przez administratora danych.	
4		2018-05-28 4/2018			Zgodnie z zakresem określonym przez administratora danych.	
5		2018-05-28 5/2018			Zgodnie z zakresem określonym przez administratora danych.	
6		2018-05-28 6/2018			Zgodnie z zakresem określonym przez administratora danych.	
7		2018-05-28 7/2018			Zgodnie z zakresem określonym przez administratora danych.	
8		2018-05-28 8/2018			Zgodnie z zakresem określonym przez administratora danych.	
9		2018-05-28 9/2018			Zgodnie z zakresem określonym przez administratora danych.	
10		2018-05-28 10/2018			Zgodnie z zakresem określonym przez administratora danych.	
11		2018-05-28 11/2018			Zgodnie z zakresem określonym przez administratora danych.	
12		2018-05-28 12/2018			Zgodnie z zakresem określonym przez administratora danych.	
13		2018-05-28 13/2018			Zgodnie z zakresem określonym przez administratora danych.	
14		2018-05-28 14/2018			Zgodnie z zakresem określonym przez administratora danych.	

16. Załącznik nr 3 - rejestr naruszeń

Wzór ewidencji naruszeń bezpieczeństwa.

Lp.	Data naruszenia	Tytuł	Opis naruszenia	Kategorie danych	Skutki naruszenia

1. **Ryzyko czynności przetwarzania**

Kryteria oceny skutków dla ochrony danych	
Art. 35 ust. 3 RODO:	
Grupa robocza art. 29 (WP 248 rev.01)	
Mechanizmy kontrolne	
Przejrzystość informacji i ułatwienie wykonywania praw:	
Źródła, sposób pozyskania oraz jakość danych:	

Zidentyfikowane aktywa

Aktywa nie zostały zdefiniowane.

Zidentyfikowane zabezpieczenia

Zabezpieczenia nie zostały zdefiniowane.

Scenariusze zdarzeń

Scenariusze zdarzeń nie zostały zdefiniowane.

być zabezpieczone przed utratą danych spowodowaną awarią zasilania poprzez stosowanie specjalnych urządzeń podtrzymujących zasilanie i eliminujących zakłócenia sieci zasilającej.

5. Komputery przenośne oraz inne mobilne nośniki danych osobowych powinny być zabezpieczone ochroną kryptograficzną – powinny być zaszyfrowane.

VIII. Sposób zabezpieczenia systemu przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.

1. Administrator danych zapewnia ochronę antywirusową oraz zarządza systemem wykrywającym i usuwającym wirusy i inne niebezpieczne kody.
2. System antywirusowy jest skonfigurowany w sposób zapewniający na bieżąco skanowanie wszystkich informacji przetwarzanych w systemie, a zwłaszcza poczty elektronicznej i stron internetowych.
3. System antywirusowy musi mieć aktywną funkcję automatycznej aktualizacji wzorców wirusów.
4. W przypadkach wystąpienia infekcji użytkownik powinien niezwłocznie powiadomić o tym fakcie Administratora danych.
5. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, należy skorzystać z pomocy specjalistów.
6. Użytkownicy systemu mają również obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, który chcą wykorzystać.

IX. Przesyłanie danych poza obszar przetwarzania

1. Urządzenia i nośniki zawierające dane osobowe, przekazywane poza obszar przetwarzania zabezpiecza się w sposób zapewniający poufność i integralność tych danych, w szczególności poprzez zastosowanie ochrony kryptograficznej.
2. W wypadku przesyłania danych osobowych przez sieć internetową pocztą elektroniczną należy każdy z załączników zabezpieczyć ochroną kryptograficzną poprzez nadanie hasła odczytu. Hasło należy przesłać lub podać odbiorcy w innej przesyłce, a najlepiej z wykorzystaniem innych metod komunikacji (tel., faks, bezpośrednia rozmowa).
3. Zabrania się przekazywania danych przez aplikacje internetowe nie wykorzystujące odpowiedniego protokołu szyfrowania (adres internetowy musi być poprzedzony zapisem „https").

X. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

1. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

- likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
- przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,
- naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem specjalisty.

Instalacji, konserwacji oraz napraw sprzętu komputerowego dokonują pracownicy firm upoważnionych przez Administratora danych.

2. Instalacji, konserwacji oraz napraw sprzętu komputerowego dokonują pracownicy firm

użytkowników systemu.

4. Za proces tworzenia kopii programów i narzędzi programowych oraz danych konfiguracyjnych systemu odpowiedzialny jest pracownik wyznaczony przez Administratora danych lub administrator danego systemu. Kopie przechowywane są w zamkniętej szafie w wydzielonym i zabezpieczonym pomieszczeniu.
5. Kopie awaryjne mogą być sporządzane automatycznie lub manualnie z wykorzystaniem specjalistycznych urządzeń do wykonywania kopii lub standardowych narzędzi oferowanych przez stacje robocze.
6. Kopie baz danych gromadzonych na serwerach wykonywane są przez administratora serwera co najmniej raz w tygodniu, zapisywane na dysk sieciowy lub zewnętrzne nośniki danych i przechowywane przez okres 30 dni, a następnie usuwane. Ostatnia kopia, przed usunięciem, jest zapisywana na przenośną pamięć zewnętrzną i przechowywana w zamkniętej szafie.
7. Kopie zbiorów danych osobowych zlokalizowanych na komputerach lokalnych wykonywane są przez poszczególnych użytkowników ostatniego dnia każdego miesiąca i zapisywane na dyskach lokalnych w ustalonej z Administratorem danych lokalizacji lub zapisywane na nośnikach zewnętrznych.
8. Nośniki, na których są przechowywane kopie danych osobowych powinny być wyraźnie oznaczone.
9. Za bezpieczeństwo kopii awaryjnych przetwarzanych lokalnie odpowiadają poszczególni użytkownicy systemu, którzy je wykonali. Kopie usuwa się niezwłocznie po ustaniu ich użyteczności w sposób uniemożliwiający odtworzenie danych.
10. Osoba upoważniona przez Administratora danych wykonuje okresowe testy odtworzeniowe kopii awaryjnych.
11. Zewnętrzne nośniki kopii awaryjnych, które zostały wycofane z użycia, podlegają zniszczeniu po usunięciu danych osobowych, w odpowiednim urządzeniu niszczącym.
12. Użytkownik tworzy wydruki związane z przetwarzaniem danych osobowych wyłącznie w zakresie i ilości niezbędnej dla celów służbowych w uzgodnieniu z przełożonym.
13. Wszystkie dokumenty, zestawienia i wydruki zawierające dane osobowe powinny być chronione przed dostępem osób nieupoważnionych. Użytkownik przechowuje je w zamkniętej szafie w pomieszczeniu zabezpieczonym przed nieuprawnionym dostępem.

VII. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji.

1. Nośniki danych oraz programy służące do przetwarzania danych osobowych, a także dane konfiguracyjne systemu informatycznego, przechowywane są w odpowiednio zabezpieczonym pomieszczeniu.
2. Dane osobowe mogą być przetwarzane na serwerach, a także na dyskach lokalnych komputerów w lokalizacji ustalonej z Administratorem danych. Zabrania się gromadzenia danych osobowych na innych, nie autoryzowanych nośnikach.
3. W uzasadnionych przypadkach, za zgodą Administratora danych, dane osobowe można przetwarzać na zewnętrznych nośnikach informacji.
4. Serwery oraz komputery, na których odbywa się przetwarzanie danych osobowych, powinny

7. Hasła najwyższego poziomu, którymi dysponuje Administrator danych gromadzone są w zamkniętej kopercie.
8. Hasła użytkowników generuje administrator danego systemu i przekazuje użytkownikowi w bezpieczny sposób.
9. Po zapoznaniu się z loginem i hasłem użytkownik zobowiązany jest do ich zniszczenia w odpowiednim urządzeniu niszczącym.
10. Hasło nie może być zapisywane i przechowywane.
11. Użytkownik nie może udostępniać identyfikatora oraz haseł osobom trzecim.

V. Procedury rozpoczęcia, zawieszenia i zakończenia pracy.

1. Każdy pracownik korzystający z systemu informatycznego przystępując do pracy powinien podać swoje dane dostępu do komputera i systemu, tj. identyfikator i hasło.
2. Zawieszenie pracy polega na opuszczeniu stanowiska pracy bez wylogowania się i jest dopuszczalne tylko w przypadku pozostania w pomieszczeniu. Użytkownik jest zobowiązany w takiej sytuacji do włączenia wygaszacza ekranu odblokowywanego hasłem.
3. Zakończenie pracy w systemie następuje poprzez prawidłowe, wymagane przez daną aplikację oraz system operacyjny, wykonanie czynności kończących. Niedopuszczalne jest zakończenie pracy poprzez wyłączenie napięcia zasilającego bez pełnej procedury zamknięcia.
4. Ekrany monitorów stanowisk komputerowych, na których odbywa się przetwarzanie danych osobowych powinny być w miarę możliwości tak umieszczone, aby uniemożliwić wgląd w dane osobom postronnym przebywającym w pomieszczeniu oraz powinny automatycznie się wyłączać poprzez stosowanie wygaszaczy ekranowych uruchamiających blokadę pracy na komputerze.
5. Osoba przetwarzająca dane osobowe w przypadku konieczności opuszczenia pomieszczenia, obowiązana jest prawidłowo, zgodnie z instrukcją obsługi systemu, zakończyć pracę w systemie.
6. Czas rozpoczynania i kończenia pracy w systemach sieciowych, w tym systemach przetwarzających dane osobowe, określa Regulamin Pracy.
7. Konieczność pracy w aplikacjach sieciowych w godzinach innych, niż określone w Regulaminie Pracy, powinna być zgłoszona Administratorowi danych.
8. Administrator danego systemu monitoruje logowanie oraz wylogowanie się użytkowników oraz nadzoruje zakres przetwarzanych przez nich danych.

VI. Procedury tworzenia kopii awaryjnych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

1. Dane osobowe zabezpiecza się poprzez wykonywanie kopii awaryjnych.
2. Ochronie poprzez wykonanie kopii podlegają także programy i narzędzia programowe służące przetwarzaniu danych.
   Kopie programów i narzędzi wykonywane są zaraz po instalacji oraz po każdej aktualizacji na zewnętrznych, elektronicznych nośnikach informacji.
3. Zabezpieczeniu poprzez wykonywanie kopii awaryjnych podlegają także dane konfiguracyjne systemu informatycznego przetwarzającego dane osobowe, w tym uprawnienia

- umożliwiania dostępu do zasobów wewnętrznej sieci informatycznej oraz sieci Internetowej osobom nieuprawnionym,
- używania komputera bez zainstalowanego oprogramowania antywirusowego.

III. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.

1. Użytkowników systemu informatycznego tworzy oraz usuwa podmiot lub osoba upoważniona przez Administratora danych do obsługi systemu informatycznego, na polecenie Administratora danych.
2. Do przetwarzania danych osobowych zgromadzonych w systemie informatycznym jak również w rejestrach tradycyjnych wymagane jest upoważnienie.
3. Wprowadza się rejestr osób upoważnionych do przetwarzania danych osobowych, który stanowi do niniejszej dokumentacji.
4. Uprawnienia do pracy w systemie informatycznym odbierane są czasowo, poprzez zablokowanie konta w przypadku:
   - nieobecności pracownika w pracy trwającej dłużej niż 21 dni kalendarzowych,
   - zawieszenia w pełnieniu obowiązków służbowych,
   - dostrzeżeniu zdarzeń zagrażających bezpieczeństwu informacji tj. próbie naruszenia integralności systemu lub bazy danych w tym systemie, jakości danych w systemie lub innego odstępstwa od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację,
   - zmianie pracownika na stanowisku komputerowym.
5. Uprawnienia do przetwarzania danych osobowych odbierane są trwale w przypadku ustania stosunku pracy.
6. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia nawet w przypadku ustania stosunku pracy.

IV. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem.

1. System informatyczny przetwarzający dane osobowe wykorzystuje mechanizm identyfikatora i hasła jako narzędzi umożliwiających bezpieczne uwierzytelnienie.
2. Użytkownik posiadający upoważnienie do przetwarzania danych osobowych powinien posiadać hasła do systemu operacyjnego oraz osobne do baz danych osobowych i aplikacji.
3. Hasło składa się z co najmniej ośmiu znaków, zawiera co najmniej jedną małą i wielką literę, jedną cyfrę lub jeden znak specjalny.
4. Hasło nie powinno zawierać żadnych informacji, które można skojarzyć z użytkownikiem komputera (imiona najbliższych, daty urodzenia, inicjały, itp.) i nie może być sekwencją kolejnych znaków klawiatury.
5. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieupoważniona, użytkownik zobowiązany jest do zgłoszenia tego faktu Administratorowi danych i do natychmiastowej zmiany hasła.
6. Zmianę hasła należy dokonywać nie rzadziej niż co 90 dni.

22. Załącznik nr 8 – instrukcja zarządzania systemem informatycznym

I. Charakterystyka system

1. Sieć informatyczną, w której przetwarzane są dane osobowe stanowią wszystkie pracujące obecne i przyszłe serwery, komputery stacjonarne i przenośne, a także urządzenia peryferyjne i sieciowe.
2. Sygnał internetowy dostarczany jest przez usługodawcę internetowego i odpowiednio zabezpieczony.
3. System zabezpieczony jest oprogramowaniem antywirusowym zainstalowanym na każdym stanowisku oraz zasilaczami awaryjnymi utrzymującymi stałe zasilanie.

II. Ogólne zasady pracy w systemie informatycznym

1. Administrator danych odpowiada za korygowanie niniejszej instrukcji w przypadku uzasadnionych zmian w przepisach prawnych dotyczących przetwarzania danych osobowych w systemach informatycznych, jak również zmian organizacyjno-funkcjonalnych.
2. Przetwarzanie danych w systemie informatycznym może być realizowane wyłącznie poprzez dopuszczone przez Administratora danych do eksploatacji licencjonowane oprogramowanie.
3. Administrator danych prowadzi ewidencję oprogramowania w ramach aktywów gromadzonych w zakresie każdej czynności przetwarzania.
4. Do eksploatacji dopuszcza się systemy informatyczne wyposażone w:
   - mechanizmy kontroli dostępu umożliwiające autoryzację użytkownika, za wyjątkiem narzędzi biurowych,
   - mechanizmy ochrony poufności, dostępności i integralności informacji, z uwzględnieniem potrzeby ochrony kryptograficznej,
   - mechanizmy umożliwiające wykonanie kopii bezpieczeństwa oraz archiwizację danych, niezbędne do przywrócenia prawidłowego działania systemu po awarii,
   - urządzenia niwelujące zakłócenia i podtrzymujące zasilanie,
   - mechanizmy monitorowania w celu identyfikacji i zapobiegania zagrożeniom, w szczególności pozwalające na wykrycie prób nieautoryzowanego dostępu do informacji lub przekroczenia przyznanych uprawnień w systemie,
   - mechanizmy zarządzania zmianami.

5. Użytkownikom zabrania się:

   - korzystania ze stanowisk komputerowych podłączonych do sieci informatycznej poza godzinami i dniami pracy bez zgody Administratora danych,
   - udostępniania stanowisk roboczych osobom nieuprawnionym,
   - wykorzystywania sieci komputerowej w celach innych niż wyznaczone przez Administratora danych,
   - samowolnego instalowania i używania programów komputerowych,
   - korzystania z nielicencjonowanego oprogramowania oraz wykonywania jakichkolwiek działań niezgodnych z ustawą o ochronie praw autorskich,

Art. 13 – klauzula ze zgodą jako podstawą

Zgodnie z art. 13 ust. 1 i 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. informuję Panią/Pana, że:

- administratorem Pani/Pana danych jest..... z siedzibą w .....;
- naszym inspektorem ochrony danych jest .....i można skontaktować się z nim/nią przez e- mail.....;
- celem przetwarzania Pani/Pana danych jest....., a podstawą prawną przetwarzania jest Pani/Pana zgoda, jednocześnie przysługuje Pani/Panu prawo do cofnięcia zgody w dowolnym momencie, jednak bez uszczerbku dla przetwarzania, którego dokonano przed cofnięciem zgody;
- podanie danych jest dobrowolne i nie jest Pani/Pan zobowiązana/y podać dane osobowe, a konsekwencjami niepodania danych są*: .....;
- odbiorcami Pani/Pana danych są:.....;
- Pani/Pana dane będą przechowywane do/przez*:.....;
- przysługuje Pani/Panu prawo do żądania dostępu do swoich danych,do ich sprostowania, do usunięcia, do ograniczenia lub sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych;
- może Pani/Pan wnieść skargę do organu nadzorczego, jeśli uważa Pani/Pan przetwarzanie Pani/Pana danych narusza Pani/Pana prawa lub rozporządzenie;
- * w oparciu o Pani/Pana dane podejmowane są zautomatyzowane decyzje (w tym profilowanie*), co oznacza, że:....., a przewidywane kosekwencje to: .....

* niepotrzebne skreślić

21. Załącznik nr 7 wzór obowiązku informacyjnego

Art. 13 – klauzula ogólna

Zgodnie z art. 13 ust. 1 i 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. informuję Panią/Pana, że:

- administratorem Pani/Pana danych jest..... z siedzibą w .....;
- naszym inspektorem ochrony danych jest .....i można skontaktować się z nim/nią przez e- mail.....
- celem przetwarzania Pani/Pana danych jest ....., a podstawą prawną przetwarzania jest.....
- podanie danych jest wymogiem ustawowym/wymogiem umownym/warunkiem zawarcia umowy/dobrowolne* i jest/nie jest* Pani/Pan zobowiązana/y podać dane osobowe, a konsekwencjami niepodania danych są*:.....
- odbiorcami Pani/Pana danych są: .....,
- Pani/Pana dane będą przechowywane do/przez*: .....
- przysługuje Pani/Panu prawo do żądania dostępu do swoich danych, do ich sprostowania, do usunięcia, do ograniczenia lub sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych;
- może Pani/Pan wnieść skargę do organu nadzorczego, jeśli uważa Pani/Pan przetwarzanie Pani/Pana danych narusza Pani/Pana prawa lub rozporządzenie;
- *w oparciu o Pani/Pana dane podejmowane są zautomatyzowane decyzje (w tym profilowanie*), co oznacza, że:..... a przewidywane konsekwencje to: .....

*niepotrzebne skreślić

20. Załącznik nr 6a – podmioty przetwarzające na podstawie umowy powierzenia

Lista podmiotów przetwarzających dane na podstawie umowy powierzenia.

Lp	Nazwa podmiotu	Dane kontaktowe
1		

rozporządzenia.

2.Sprawy wynikłe na tle niniejszej umowy rozstrzygał będzie Sąd Rejonowy według właściwości ogólnej, a na tle stosowania rozporządzenia – właściwy organ nadzorczy.

3.Zmiany umowy wymagają dla swej ważności formy pisemnej.

4.Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

ADMINISTRATOR	PODMIOT PRZETWARZAJĄCY
.....	.....

1. Administrator upoważnia podmiot przetwarzający do dalszego powierzenia danych wskazanych w § 4 ust. 1 na zasadach ogólnej lub szczegółowej pisemnej zgody.
2. Upoważnienie do dalszego powierzenia w formie ogólnej pisemnej zgody wymaga, aby:
   a. Podmiot przetwarzający przedstawił na piśmie administratorowi podwykonawcę, informując o jego: nazwie, adresie, przedmiocie i czasie trwania przetwarzania, charakterze i celu, rodzaju danych i kategorii osób oraz obowiązkach podwykonawcy.
   b. Administrator zatwierdził pisemnie podwykonawcę. Równoważną formą zatwierdzenia jest brak sprzeciwu/odpowiedzi administratora na pismo podmiotu przetwarzającego w terminie do ..... dni.
   c. Wyżej wymienione pisma stanowiły załącznik do niniejszej umowy.
3. Upoważnienie do dalszego powierzenia w formie szczegółowej pisemnej zgody wymaga, aby w niniejszej umowie zawarte zostały wszystkie informacje o podwykonawcach wymagane w § 7 ust. 2 lit. a. Klauzule te wchodzą w życie z dniem podpisania umowy.
4. Strony ustalają, że podwykonawcami, zgodnie z § 7 ust. 3, są:
   1.....
   .....
   2.....
   .....
   3.....
   .....
5. Podmiot przetwarzający zapewnia, że podwykonawcy stosują co najmniej równorzędne środki techniczne i organizacyjne ochrony jak podmiot przetwarzający.
6. Podmiot przetwarzający informuje administratora o rozwiązaniu lub wypowiedzeniu umowy przez podwykonawcę w terminie do ..... dni.
7. Podpowierzenie można oprzeć o standardowe klauzule umowne zdefiniowane przez Komisję lub organ nadzorczy bez szkody dla zapisu niniejszej umowy.

§8

Rozwiązanie umowy

1. Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy podmiot przetwarzający:
   a. pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas audytu lub inspekcji nie usunie ich w wyznaczonym terminie;
   b. przetwarza dane osobowe w sposób niezgodny z umową lub rozporządzeniem;
   c. powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody administratora danych;

§9

Postanowienia końcowe

1.W sprawach nieuregulowanych niniejszą umową zastosowanie mają przepisy kodeksu cywilnego i

§3
Charakter i cel przetwarzania

1. Charakter przetwarzania wynika z zakresu powierzonej czynności przetwarzania i dotyczy w szczególności użytych środków technicznych i organizacyjnych ochrony oraz kontaktu podmiotu przetwarzającego z osobami, których dane dotyczą. Charakter przetwarzania określa się jako:

.....
.....

2. Celem powierzenia przetwarzania czynności jest:

.....

§4
Rodzaj danych osobowych i kategorie osób, których dane dotyczą

1. Administrator powierza podmiotowi przetwarzającemu następujące rodzaje (kategorie) danych osobowych:

.....
.....

2. Wskazane rodzaje (kategorie) danych osobowych dotyczą następujących osób (jeśli różne rodzaje dotyczą różnych osób, należy dookreślić do jakich osób się odnoszą):

.....
.....

§5
Obowiązki i prawa administratora

1. Administrator ma obowiązek niezwłocznie udostępnić dane wskazane w § 4 ust. 1 podmiotowi przetwarzającemu.
2. Administrator ma obowiązek odpowiadać na żądania osób, których dane dotyczą w związku z realizowaniem ich praw z rozdziału III rozporządzenia i ma prawo prosić o pomoc podmiot przetwarzający, zgodnie z art. 28 ust. 3 lit. e) rozporządzenia.
3. Administrator ma obowiązek wywiązać się z obowiązków określonych w art. 32-36 rozporządzenia i ma prawo prosić o pomoc podmiot przetwarzający zgodnie z art. 28 ust. 3 lit. f) rozporządzenia.
4. Administrator ma prawo przeprowadzić audyt lub inspekcję podmiotu przetwarzającego osobiście lub poprzez upoważnioną do tego osobę.

§6
Obowiązki i prawa podmiotu przetwarzającego

1. Podmiot przetwarzający ma obowiązek realizować zapisy art. 28 ust. 3 rozporządzenia.
2. Podmiot przetwarzający ma prawo podpowierzyć przetwarzanie danych osobowych w trybie § 7 umowy.

§7
Podpowierzenie przetwarzania danych osobowych

19. Załącznik nr 6 – wzór umowy powierzenia przetwarzania danych

Umowa powierzenia przetwarzania danych osobowych

(zwana dalej „umową")

Zawarta w dniu ..... w ..... pomiędzy:

.....,

.....

reprezentowanym/ą przez:

.....

.... zwanym/ą dalej „administratorem" lub „administratorem danych",

a

.....,

.....

reprezentowanym/ą przez:

..... zwanym/ą dalej „podmiotem przetwarzającym".

§1

Powierzenie przetwarzania danych osobowych

1. Administrator powierza podmiotowi przetwarzającemu do przetwarzania dane osobowe w trybie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zwanego dalej rozporządzeniem.
2. Podmiot przetwarzający oświadcza, że zapewnia wystarczające gwarancje wdrożenia i stosowania odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi rozporządzenia i chroniło prawa osób, których dane dotyczą.
3. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone dane osobowe zgodnie z umową, rozporządzeniem i innymi prawami Unii oraz państw członkowskich właściwych administratorowi i podmiotowi przetwarzającemu.

§2

Przedmiot i czas trwania przetwarzania

1. Przedmiotem powierzenia jest czynność przetwarzania w zakresie operacji lub zestawu operacji podanych dalej w nawiasie:
   .....
   .....
2. Czas trwania przetwarzania czynności ustala się na nieokreślony/określony*
   od ..... do .....

upoważnionych przez Administratora danych.

3. Przeglądy i konserwacje systemu oraz nośników informacji służących do przetwarzania danych mogą być wykonywane jedynie przez osoby posiadające upoważnienie wydane przez Administratora danych lub posiadające umowy na powierzenie przetwarzania danych w zakresie konserwacji i napraw.
4. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wymaganego poziomu zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych, w szczególności poprzez bezpośredni nadzór prowadzony przez wskazane przez Administratora danych osoby.
5. Należy wykonywaćokresowy przegląd nośników danych osobowych eliminując te, które nie zapewniają odpowiedniego poziomu bezpieczeństwa oraz niezawodności.

23. Załącznik nr 9 – ewidencja aktywów

W poniższej tabeli zestawiono, sumarycznie dla wszystkich czynności przetwarzania aktywa.

Lp.	Na	Rodzaj	Wartość	Odpowiedzialność
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				
31				
32				

24. Załącznik nr 10 – ewidencja zagrożeń

W poniższej tabeli zestawiono, sumarycznie dla wszystkich czynności przetwarzania zagrożenia dla danych osobowych.

Lp	Nazwa	Rodzaj	Źródło
1	Awaria systemu klimatyzacji lub dostaw wody	Utrata podstawowych usług	Umyślne, Przypadkowe
2	Awaria urządzenia	Awarie techniczne	Przypadkowe
3	Błąd użytkowania	Naruszenie bezpieczeństwa funkcji	Przypadkowe
4	Dane z niewiarygodnych źródeł	Naruszenie bezpieczeństwa informacji	Umyślne, Przypadkowe
5	Kradzież dokumentów, urządzeń lub nośników	Naruszenie bezpieczeństwa informacji	Umyślne
6	Nieautoryzowane użycie urządzeń	Nieautoryzowane działania	Umyślne
7	Niewłaściwe funkcjonowanie	Awarie techniczne	Przypadkowe
8	Niewłaściwe funkcjonowanie urządzeń	Awarie techniczne	Przypadkowe
9	Pożar lub inna forma zniszczenia	Zjawiska fizyczne	Naturalne, Umyślne, Przypadkowe
10	Przeciążenie systemu informacyjnego	Awarie techniczne	Umyślne, Przypadkowe
11	Ujawnienie, utrata lub kradzież danych	Naruszenie bezpieczeństwa informacji	Umyślne, Przypadkowe
12	Utrata dostaw prądu	Utrata podstawowych usług	Naturalne, Umyślne, Przypadkowe
13	Zjawiska klimatyczne	Zjawiska naturalne	Naturalne
14	Zjawiska pogodowe	Zjawiska naturalne	Naturalne
15	Zniszczenie dokumentów, urządzeń lub nośników	Zjawiska fizyczne	Naturalne, Umyślne, Przypadkowe

25. Załącznik nr 11 – ewidencja podatności na zagrożenia

W poniższej tabeli zestawiono, sumarycznie dla wszystkich czynności przetwarzania możliwe do wystąpienia podatności na zagrożenia.

Lp	Nazwa	Rodzaj	Łatwość
1	Brak dokumentacji	Oprogramowanie	Wysoka
2	Brak dowodu wysłania lub odebrania wiadomości	Sieć	Średnia
3	Brak lub niewystarczająca polityka 'czystego biurka i czystego ekranu'	Organizacja	Średnia
4	Brak świadomości w zakresie bezpieczeństwa	Personel	Wysoka
5	Nieobecność personelu	Personel	Wysoka
6	Praca personelu zewnętrznego lub sprzątającego bez nadzoru	Organizacja	Średnia
7	Złe zarządzanie hasłami	Oprogramowanie	Wysoka

26. Załącznik nr 12 - widencja zabezpieczeń

W poniższej tabeli zestawiono, sumarycznie dla wszystkich czynności przetwarzania stosowane zabezpieczenia.

Lp	Nazwa	Status	Rodzaj	Podatność	Skuteczność
1	Automatyczne wylogowanie przy	Istniejące	Oprogramowanie		Wysoka
2	Logowanie do zbioru lub systemu	Istniejące	Oprogramowanie		Wysoka
3	Okresowa zmiana haseł dostępu do	Istniejące	Oprogramowanie		Średnia
4	Polityka bezpieczeństwa haseł	Istniejące	Oprogramowanie		Wysoka
5	Program antywirusowy	Istniejące	Oprogramowanie		Wysoka
6	Wygaszacz ekranu	Istniejące	Oprogramowanie		Średnia
7	Wykonywani ekopii	Istniejące	Oprogramowanie		Wysoka
8	Polityka 'czystego biurka i czystego	Istniejące	Organizacja		Wysoka
9	Raportowanie naruszeń	Istniejące	Organizacja		Wysoka
10	Regularne szacowanie	Istniejące	Organizacja		Wysoka
11	Regularny audyt	Istniejące	Organizacja		Wysoka
12	Umowy powierzenia	Istniejące	Organizacja		Wysoka
13	Polityka bezpieczeństwa	Istniejące	Personel		Wysoka
14	Rejestracja zmian dokonywanych w	Istniejące	Personel		Średnia
15	Szkolenie personelu z ochrony danych	Istniejące	Personel		Wysoka
16	Zaznajomienie personelu z obsługą	Istniejące	Personel		Średnia
17	Właściwa konfiguracja	Istniejące	Sieć		Średnia
18	Drzwi drewniane	Istniejące	Siedziba		Niska
19	Kraty lub rolety w	Istniejące	Siedziba		Wysoka
20	Sejf lub kasa pancerna	Istniejące	Siedziba		Wysoka
21	Służba ochrony poza czasem pracy	Istniejące	Siedziba		Wysoka
22	Służba ochrony poza czasem pracy	Istniejące	Siedziba		Wysoka
23	System kontroli dostępu	Istniejące	Siedziba		Wysoka

27. Załącznik nr 13 – ewidencja skutków dla osób fizycznych

Poniżej zestawiono zbiorczo mogące nastąpić skutki dla osób fizycznych, w związku z przetwarzaniem ich danych osobowych.

Lp.	Nazwa	Kategoria skutku	Wartość
1	Naruszenie dobrego imienia	Szkoda niemajątkowa	Średnia
2	Naruszenie poufności danych osobowych chronionych tajemnicą zawodową	Szkoda niemajątkowa	Średnia
3	Naruszenie prawa do ograniczenia danych	Szkoda niemajątkowa	Wysoka
4	Niedopełnienie obowiązku informacyjnego	Szkoda niemajątkowa	Wysoka
5	Niedopełnienie obowiązku informacyjnego względem osoby, której dane pozyskano z innego źródła	Szkoda niemajątkowa	Wysoka
6	Niepowiadomienie osoby, której dane dotyczą o naruszeniu ochrony danych	Szkoda niemajątkowa	Wysoka
7	Zablokowanie konta	Szkoda majątkowa	Średnia

28. Załącznik nr 14 – ewidencja wyjątków akceptacji ryzyka

Poniżej zestawiono zbiorczo wyjątki akceptacji ryzyka, które mogą być brane pod uwagę przy akceptacji ryzyk powyżej wartości progowej.

Lp.	Nazwa	Komentarz
1	Akceptacja czasowa	Akceptacja do czasu wdrożenia zalecanych zabezpieczeń
2	Powody ekonomiczne	Organizacja jest niezdolna do wdrożenia odpowiednich zabezpieczeń, a potencjalny zysk przewyższa ewentualne ryzyko.
3	Powody organizacyjne	Akceptacja ryzyka jest wymagana dla ciągłości działania organizacji lub wymusza ją struktura.
4	Powody technologiczne	Nie istnieje jeszcze dostatecznie dobry środek techniczny ochrony lub nowa technologia znacząco ułatwia przetwarzanie i nie zdarzyło się, żeby była przyczyną wysokiego ryzyka.
5	Wymagania umowy	Strony uzgodniły umownie, że będzie wymagane zaakceptowanie ryzyka i wysokiego ryzyka, gdy wystąpi w związku z przetwarzaniem.
6	Wypełnienie obowiązku prawnego lub zadania realizowanego w interesie publicznym.	W odniesieniu do art. 35 ust. 10 wskazującemu, że ocena skutków (szczegółowa analiza ryzyka) dla przetwarzania na mocy art. 6 ust 1 lit c) i e) nie jest konieczna, jeśli państwo członkowskie dokonało oceny w ramach oceny skutków regulacji, przyjmuje się, że ryzyko i wysokie ryzyko można zaakceptować, chyba że państwo członkowskie wymaga oceny skutków dla takiej operacji lub podjęcia innych działań, aby obniżyć ryzyko.

29.Załącznik nr 15 – rejestr kategorii czynności przetwarzania

ID	Kategorie przetwarzań	Środki techniczne i organizacyjne bezpieczeństwa	Administratorzy lub podmioty przetwarzające
1			
2			