Zarządzenie Nr 116 /2021
Wójta Gminy Jedwabno
z dnia 14 grudnia 2021 roku

w sprawie wprowadzenia „Polityki Bezpieczeństwa w Urzędzie Gminy Jedwabno".

Na podstawie art.24 ust.1 i ust.2 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 osobowych),

zarządza się, co następuje:

§ 1. Wprowadza się „Politykę Bezpieczeństwa w Urzędzie Gminy Jedwabno" stanowiącą załącznik Nr 1 do niniejszego zarządzenia.

§ 2. Zobowiązuje się wszystkie osoby przetwarzające dane osobowe w Urzędzie Gminy Jedwabno do przestrzegania zasad i realizacji zadań określonych w załączniku, o którym mowa w § 1.

§ 3. Tracą ważność zarządzenia Wójta Gminy Jedwabno:
- Nr 80/2018 z dnia 25.07.2018 r. w sprawie wprowadzenia „Polityki Bezpieczeństwa w Urzędzie Gminy Jedwabno";
- Nr 116/2018 z dnia 15.11.2018 r. w sprawie zmiany zarządzenia Nr 80/2018 Wójta Gminy Jedwabno z dnia 25.07.2018 r. w sprawie wprowadzenia „Polityki Bezpieczeństwa Urzędu Gminy w Jedwabnie";
- Nr 99/2020 z dnia 12.10.2020 r. w strawie wprowadzenia zmian w „Polityce Bezpieczeństwa w Urzędzie Gminy w Jedwabnie".

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

Wójt

(Sławomir Ambroziak)

Załącznik Nr 1
do zarządzenia
Nr 116/2021 Wójta Gmi
Jedwabno z dnia 14.XII.20

Polityka Bezpieczeństwa w Urzędzie Gminy Jedwabno

Zatwierdził:

Data zatwierdzenia:
14.12.2021

Wstęp

Celem dokumentu jest ustanowienie jednolitych reguł postępowania w zakresie ochrony danych osobowych. Polityka bezpieczeństwa określa zasady bezpiecznego przetwarzania oraz definiuje środki zabezpieczające przed nieuprawnionym przetwarzaniem, dostępem, ujawnieniem, utratą, nieprawidłowym wykorzystaniem lub kradzieżą danych osobowych.

Dokument ten ma zastosowanie do wszystkich przetwarzanych danych osobowych na mocy przepisów prawnych, określonych w Załączniku nr 1: Wykaz aktów prawnych. Rejestr ten powinien być aktualizowany na bieżąco w przypadku zmian prawnych, ułatwiając podejmowanie decyzji.

Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich pracowników upoważnionych do przetwarzania danych osobowych. Pojęcie pracownik oznacza w tym przypadku osobę zatrudnioną na podstawie umowy o pracę lub innej umowy cywilnoprawnej (tymczasowej lub długoterminowej), odbywającą staż lub praktyki studenckie.

W przypadku korzystania z firm zewnętrznych reguły postępowania zostały również w tym dokumencie uwzględnione.

Dane osobowe są przetwarzane w Urzędzie Gminy w Jedwabnie zarówno w sposób tradycyjny, jak i elektronicznie. Ze względu na zasadnicze różnice w zastosowanych mechanizmach zabezpieczających, wyodrębniono dwa dokumenty podrzędne, które szczegółowo określają zasady ochrony danych osobowych przetwarzanych w formie papierowej (Załącznik nr 2: Polityka bezpieczeństwa danych osobowych przetwarzanych w zbiorach papierowych) i w systemach informatycznych (Załącznik nr 3: Polityka bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych stanowiąca odwołanie do Systemu Zarządzania Bezpieczeństwem Informacji). Środki ochrony danych osobowych, na które ma wpływ sposób przetwarzania tych danych, zostały określone w niniejszym dokumencie, w tym zasady szyfrowania, anonimizacji i pseudonimizacji.

Dokument Polityki Bezpieczeństwa został opracowany w oparciu o wytyczne zawarte w następujących aktach prawnych:

1) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenie dyrektywy 95/46 WE (Ogólne rozporządzenie o ochronie danych);
2) Obwieszczenie Prezesa Rady Ministrów z dnia 14 stycznia 2016 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych
3) Ustawa o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000).
4) Dz. U. z 2018 r. poz. 1560 - Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Używane skróty.

1. **Administrator danych, ADO** – Wójt Gminy Jedwabno (organ, jednostka organizacyjna, podmiot lub osoba, decydująca o celach i środkach przetwarzania danych osobowych),
2. **IOD** – Inspektor Ochrony Danych Osobowych;
3. **Pełnomocnik** – osoba upoważniona do której zadań należy wdrożenie i nadzór nad prawidłową realizacją w imieniu ADO Polityki Bezpieczeństwa obowiązującej w jednostce organizacyjnej w przypadku niepowołania IOD;
4. **ASI** – Administrator Systemów Informatycznych, osoba upoważniona do zarządzania systemem informatycznym;
5. **Rozporządzenie** – Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024 ze. zm.);
6. **Rozporządzenie RODO, RODO** - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenie dyrektywy 95/46 WE (Ogólne rozporządzenie o ochronie danych);
7. **Przetwarzanie danych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie;
8. **Poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom;
9. **Użytkownik** – osoba upoważniona do przetwarzania danych osobowych;
10. **System informatyczny** – system przetwarzania danych w Urzędzie Gminy w Jedwabnie wraz z zasobami ludzkimi, technicznymi oraz finansowymi, który dostarcza i rozprowadza informacje;
11. **Zabezpieczenie systemu informatycznego** – należy przez to rozumieć wdrożenie stosowanych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem, ujawnieniem a także ich utratą;

12. **Właściciel Biznesowy, Właściciel** - osoba zarządzająca komórką odpowiadająca za ochronę danych osobowych przetwarzanych w podległym sobie obszarze lub komórce organizacyjnej, w tym za dany projekt biznesowy, działanie lub proces, który wiąże się z przetwarzaniem danych osobowych;
13. **Dane Osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. 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. Osobom fizycznym mogą zostać przypisane identyfikatory internetowe – takie jak adresy IP, identyfikatory plików cookie – generowane przez ich urządzenia, aplikacje, narzędzia i protokoły, czy też inne identyfikatory. Aby stwierdzić, czy dana osoba jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby, w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej, przy czym należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas potrzebny do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny;
14. **Przepisy z zakresu ochrony danych osobowych** – oznacza obowiązujące regulacje z zakresu ochrony danych osobowych, w tym RODO;
15. **Odbiorca danych** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Odbiorcą jest również Przetwarzający;
16. **Organ Nadzorczy** – niezależny organ publiczny, o którym mowa w art. 51 RODO, odpowiedzialny za monitorowanie stosowania RODO, w tym Prezes Urzędu Ochrony Danych Osobowych;
17. **Podmiot Danych** – osoba, której dane dotyczą.
18. **SZBI** - Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych

Zasady zarządzania informacją.

Każdy pracownik powinien być zapoznany z zasadami oraz z kompletnymi i aktualnymi procedurami ochrony informacji. Prezentowane poniżej reguły są podstawą realizacji Polityki Bezpieczeństwa:

- Zasada uprawnionego dostępu – każdy pracownik przechodzi szkolenie z zasad ochrony informacji, spełnia kryteria dopuszczenia do informacji i podpisuje stosowne oświadczenie o zachowaniu poufności.
- Zasada przywilejów koniecznych – każdy pracownik posiada prawa dostępu do informacji, ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań.
- Zasada wiedzy koniecznej – każdy pracownik posiada niezbędną wiedzę o systemie, do którego ma dostęp tylko w zakresie realizacji powierzonych mu zadań.
- Zasada świadomości uczestniczą w tym procesie poprzez regularne szkolenia.
- Zasada indywidualnej odpowiedzialności – każdy pracownik odpowiada za bezpieczeństwo poszczególnych elementów systemu zarządzania bezpieczeństwem informacji.
- Zasada obecności koniecznej – prawo przebywania w określonych miejscach mają tylko osoby upoważnione.
- Zasada stałej gotowości – niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających.
- Zasada najsłabszego ogniwa – poziom bezpieczeństwa wyznacza najsłabiej zabezpieczony element, którym najczęściej jest człowiek (pracownik).
- Zasada kompletności – zabezpieczenie jest skuteczne tylko wtedy, gdy stosuje się podejście kompleksowe, uwzględniające wszystkie stopnie i ogniwa ogólnie pojętego procesu przetwarzania informacji.
- Zasada ewolucji – każdy system musi ciągle dostosowywać mechanizmy wewnętrzne do zmieniających się warunków zewnętrznych.
- Zasada świadomej konwersacji – nie zawsze i wszędzie trzeba mówić, co się wie, ale zawsze i wszędzie trzeba wiedzieć co, gdzie i do kogo się mówi.
- Zasada zamkniętego pomieszczenia – ostatnia osoba wychodząca z pomieszczenia na zakończenie dnia pracy jest zobowiązana zamknąć drzwi na klucz. Niedopuszczalne jest

pozostawienie otwartych pomieszczeń w godzinach pracy, gdy nikogo upoważnionego nie ma w środku.

- Zasada nadzorowanych dokumentów – po godzinach pracy w zamkniętych szafach lub biurkach powinny być przechowywane wszystkie dokumenty, które zostały uznane za informacje istotne dla działania Urzędu Gminy w Jedwabnie.
- Zasada czystego biurka – należy unikać pozostawiania dokumentów na biurku bez opieki. Po zakończeniu pracy należy uprzątnąć biurko z dokumentów papierowych, płyt CD oraz innych nośników danych.
- Zasada czystego ekranu – każdy komputer musi mieć ustawiony wygaszacz ekranu. Wygaszacz powinien włączać się automatycznie po 15 minutach bezczynności użytkownika. Użytkownik powinien zablokować komputer przed opuszczeniem stanowiska pracy, a w przypadku dłuższej nieobecności – wylogować się z systemu. Po zakończonym dniu komputer powinien zostać wyłączony.
- Zasada czystych drukarek – dokumenty zawierające informacje chronione w Urzędzie powinny być zabierane z drukarek natychmiast po wydrukowaniu. W przypadku nieudanej próby wydrukowania dokumentu na użytkowniku spoczywa obowiązek ustalenia miejsca przesłania dokumentu do drukarki, adekwatnie do zasady indywidualnej odpowiedzialności.
- Zasada czystego kosza – dokumenty papierowe z wyjątkiem materiałów promocyjnych, marketingowych i informacyjnych powinny być niszczone w sposób uniemożliwiający ich odczytanie.

Sposoby przetwarzania informacji.

Wszystkie informacje przetwarzane są zarówno w sposób tradycyjny, jak i w formie elektronicznej przy użyciu systemów informatycznych. W dokumentacji terminy *system informatyczny*, *aplikacja* i *oprogramowanie* są tożsame i stosuje się je wymiennie. Należy jednak pamiętać, że przetwarzanie danych w systemie informatycznym oznacza równoczesne zaangażowanie zasobów organizacyjnych, sprzętowych i programowych. Zgodnie z tym pełna definicja systemu informatycznego to zespół współpracujących ze sobą urządzeń, procedur przepływu informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Zarządzanie warstwą techniczną systemu informatycznego należy do zadań ASI lub firmy zewnętrznej z którą zawarto umowę na realizację usług informatycznych.

Zasoby sprzętowe systemu informatycznego zawiera Załącznik nr 4: Inwentaryzacja zasobów IT, obejmujący zarówno sprzęt komputerowy (serwery, komputery PC, laptopy), aktywne urządzenia sieciowe jak i inne środki przetwarzania (drukarki, skanery, urządzenia wielofunkcyjne, kserokopiarki, faksy, pendrive, dyski zewnętrzne). W przypadku zastosowania do celów inwentaryzacyjnych specjalistycznego oprogramowania, załącznik wskazuje minimum informacji, które powinien on przetwarzać. W celu prawidłowego zarządzania infrastruktura informatyczną, urządzeniami, sieciami oraz oprogramowaniem ADO ma prawo powołać Administratora Systemów Informatycznych (ASI). Wzór powołania stanowi Załącznik nr 17: Upoważnienie dla ASI. Rolę ASI może pełnić firma, z którą zawarto umowę.

Inwentaryzacja zasobów informacyjnych.

Zasoby informacyjne wymienione zostały w Załączniku nr 5: Inwentaryzacja zasobów informacyjnych, gdzie uszczegółowiono: jakie kategorie informacji są przetwarzane i w jaki sposób, jaki jest cel oraz podstawa prawna przetwarzania, a także w jakim miejscu oraz przez jaki okres czasu dane będą przechowywane. W przypadku zmiany któregokolwiek z elementów załącznik powinien być zaktualizowany.

Umowy powierzenia przetwarzania danych osobowych.

1. Ustawa o ochronie danych osobowych przewiduje m.in. możliwość powierzenia przetwarzania danych, ich przekazania czy udostępniania zewnętrznym podmiotom. Może się to odbywać wyłącznie na drodze umowy, w której należy określić zbiór, który zostanie przekazany, cel tego przekazania, zakres planowanego przetwarzania danych przez inny podmiot oraz wskazać gwarancje prawidłowego przetwarzania.

2. Wszelkie umowy dotyczące przekazania danych osobowych zawiera Administrator Danych.

3. Wzór ewidencji podmiotów, z którymi została zawarta umowa do przetwarzania danych stanowi Załącznik nr 7: Ewidencja podmiotów, z którymi została zawarta umowa do przetwarzania danych lub mają dostęp do obszaru przetwarzania danych.

Obszar, w którym przetwarzane są dane osobowe.

Przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach biurowych w siedzibie Urzędu Gminy w Jedwabnie znajdującej się w Jedwabnie przy ulicy Warmińskiej 2. Pomieszczenia, w których przetwarzane są dane osobowe zawiera Załącznik nr 8: Obszar przetwarzania danych.

Organizacja pracy przy przetwarzaniu danych osobowych i zasady przetwarzania.

Wykaz pracowników uprawnionych do przetwarzania danych osobowych, znajduje się w ***Załączniku nr 9. Ewidencja osób upoważnionych do przetwarzania danych***.

- przetwarzać dane osobowe mogą jedynie pracownicy, którzy posiadają stosowne upoważnienie przyznane przez Administratora Danych Osobowych, wzór stanowi dokument: Upoważnienie do przetwarzania danych (załącznik nr 18).
- w trakcie przetwarzania danych osobowych, pracownik jest osobiście odpowiedzialny za bezpieczeństwo powierzonych mu danych, co potwierdza oświadczeniem zawartym w Załączniku nr 18.

- w trakcie przetwarzania danych osobowych, pracownik winien dbać o należyte ich zabezpieczenie przed możliwością wglądu bądź zmiany przez osoby do tego celu nieupoważnione,
- po zakończeniu przetwarzania danych pracownik winien należycie zabezpieczyć dane osobowe przed możliwością dostępu do nich osób nieupoważnionych.

Osoby odpowiedzialne za ochronę danych osobowych tworzą rejestr czynności przetwarzania. Wzór rejestru stanowi załącznik nr 10.

W art. 30 RODO, przewidziane są następujące kategorie czynności przetwarzania: 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. W przypadku działania jako podmiot, któremu inny administrator powierzył przetwarzanie w trybie art. 28 RODO prowadzony jest rejestr wszystkich kategorii czynności przetwarzania dokonywanych na rzecz każdego z administratorów w formie dokumentu stanowiącego Załącznik 10a. Wzór rejestru wszystkich kategorii czynności przetwarzania. Wójt Gminy Jedwabno jako Administrator Danych oraz jako Procesor zobowiązany jest do opracowania (w formie dokumentacji) oraz wdrażania zasad i reguł postępowania związanych z bezpieczeństwem przetwarzania danych, w szczególności osobowych, a także do monitorowania przestrzegania zasad i procedur określonych w tejże dokumentacji. Przyjęte środki techniczne oraz organizacyjne służące ochronie prywatności są regularnie przeglądane oraz uaktualniane.

Wobec powyższego, kategorie czynności można podzielić na dwie główne grupy: wewnętrzne (co robimy z danymi w zbiorze) oraz zewnętrzne (ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie), które dotyczą ujawniania, rozpowszechniana lub inne rodzaju udostępniania. Dla zachowania spójności zarządzania w/w kategoriami czynności przyjęto podział na następujące typy: powierzenie, udostępnienie, przekazanie do państwa trzeciego, przyjęcie powierzenia (administrator powierzył nam przetwarzanie), wewnętrzne – czynności, które przeprowadzamy w ramach konkretnego zbioru.

Szacowanie ryzyka i wybór zabezpieczeń.

ADO przeprowadza ogólne szacowanie ryzyka, która polega na przyporządkowaniu do wyników inwentaryzacji z części pierwszej i drugiej potencjalnych zagrożeń dla bezpieczeństwa danych osobowych wraz z zapisem i uzasadnieniem decyzji o konkretnych działaniach związanych z zabezpieczeniem informacji.

ADO zobowiązany jest do uwzględnienia możliwości nieuprawnionego lub przypadkowego: zniszczenia, utraty, zmodyfikowania, nieuprawnionego ujawnienia, nieuprawnionego dostępu. Szacowanie ryzyka określane jest w oparciu o procedurę, opisaną w Załączniku 11: Ogólne szacowanie ryzyka. W wyniku szacowania ryzyka powstanie dokument, który powinien być cyklicznie sporządzany, nie rzadziej niż raz w roku oraz przy każdej zmianie czynników powodujących zagrożenie. Możliwe jest wykorzystanie innych metod szacowania.

Naruszenie danych.

W przypadku „naruszenia ochrony danych osobowych" administrator ma obowiązek niezwłocznie (w miarę możliwości w ciągu 72 godzin) od uzyskania wiedzy o przypadku naruszenia poinformować o nim GIODO. Przez naruszenie ochrony danych osobowych rozporządzenie rozumie „naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych". Definicja naruszenia obejmuje nie tylko przypadki włamań do systemów informatycznych, ale tak prozaiczne zdarzenia, jak np. zgubienie laptopa czy wysłanie e-maila do niewłaściwej osoby (o ile oczywiście prowadzą do nieuprawnionego dostępu do danych osobowych).
W przypadku uzyskania informacji o możliwości naruszenia bezpieczeństwa danych stosuje się Procedurę postępowania w przypadku naruszenia bezpieczeństwa danych (Załącznik nr 15) oraz uzupełnia Rejestr naruszeń ochrony danych osobowych (Załącznik nr 16).

Każde stwierdzone naruszenie musi zostać odnotowane w wewnętrznym rejestrze naruszeń a te naruszenia, które zostały zaklasyfikowane jako chrakteryzujące się większym niż niski stopniem powagi naruszenia w rozumieniu procedury opisanej w Procedurze postępowania w

przypadku naruszenia bezpieczeństwa danych muszą zostać zgłoszone do Prezesa Urzędu Ochrony Danych Osobowych niezwłocznie – nie później niż w ciągu 72 godzin od stwierdzenia naruszenia. Naruszenia, które zostały zaklasyfikowane jako chrakteryzujące się wysokim lub bardzo wysokim stopniem powagi naruszenia muszą zostać zakomunikowane osobom, których danych one dotyczyły, oceny dokonuje się na podstawie dokumentu w załączniku 15.

Monitorowanie i sprawdzenie przestrzegania przyjętych procedur ochrony danych osobowych.

Osoba wykonująca funkcję ADO najpóźniej do 30 stycznia każdego roku kalendarzowego przygotowuje harmonogram sprawdzeń, który zawiera:

- terminy przeprowadzenia sprawdzeń
- określenie zakresu sprawdzeń przeprowadzanych w konkretnych terminach

Przygotowany harmonogram sprawdzeń zatwierdzany jest jako obowiązujący dokument najpóźniej do 15 lutego każdego roku kalendarzowego. Założenia oraz wzory dokumentów zawiera Załącznik nr 20: Monitorowanie i sprawdzenie.

Osoby upoważnione do przetwarzania danych osobowych nie są informowane o sprawdzeniach przed ich rozpoczęciem. Dostępny dla pracowników jest dokument Załącznik nr 21: Wyciąg z procedur ochrony danych.

Szkolenia

Każdy pracownik biorący udział w procesie przetwarzania danych osobowych przechodzi obowiązkowe szkolenie przed rozpoczęciem pracy oraz przynajmniej jeden raz w roku. Program szkolenia musi uwzględniać aktualną Politykę Bezpieczeństwa. Ze szkolenia sporządza się protokół, na którym pracownik własnym podpisem potwierdza fakt przeszkolenia. Celem szkoleń jest osiągnięcie stanu, w którym każdy pracownik będzie w stanie zidentyfikować, kiedy dochodzi do przetwarzania danych osobowych. Program szkolenia powinien zawierać przynajmniej takie elementy jak: omówienie ogólne RODO, omówienie aktualnej Ustawy o Ochronie Danych Osobowych, zasady zarządzania informacją,

procedury postępowania z dokumentacją tradycyjną (papierową) i elektroniczną w organizacji. Wzory dokumentów zawiera Załącznik nr 22: Szkolenia.

Realizacja Praw.

Realizacja praw osób, przedstawiony w załączniku nr 24, w formie papierowej zawiera wszystkie elementy niezbędne do wykonania żądania. Ważnym jest przy tym fakt, że każdorazowo decyzję taką należy zweryfikować pod kątem poprawności żądania. Wydaje się słusznym przyjęcie założenia, że potwierdzenie zgody na przetwarzanie danych w formie papierowej, powinno implikować tożsame (co do medium) wystąpienie o realizację praw, ze względu na występujące w formie papierowej dane, potwierdzenia czy podpisy. RODO nie precyzuje medium a jedynie wskazuje na możliwość skorzystania z przysługującego prawa. Tym samym wydaje się zasadne przedstawienie żądania usunięcia danych na takim samym medium na jakim wystąpiła zgoda na ich przetwarzanie. Decyzję w tej kwestii podejmuje administrator.

Jednym z newralgicznych elementów procesów ochrony danych osobowych jest zarządzanie cyklem życia danych. Wytyczne i zasady zawarte są w Załączniku nr 25: Zarządzanie cyklem życia danych osobowych. Jednym z elementów jest retencja danych której przykład zawarty jest w Załączniku 19: Retencja.

Ostatnim z elementów cyklu życia danych jest ich niszczenie. Wytyczne do tego procesu zawiera Załącznik nr 26: Niszczenie zbiorów danych osobowych.

Istotnym dla bezpieczeństwa organizacji jest zapewnienie odpowiedniej jej ochrony w innych aspektach: BHP, ochrony p. poż., szeroko pojętej ochrony czy problemów środowiskowych. Polityka nie zawiera szczegółowych opisów realizacji tych aspektów. Wskazane jest odwołanie się przy realizacji oceny bezpieczeństwa do aktów prawa wewnętrznego które je dookreślają.

Polityka bezpieczeństwa podlega okresowym przeglądom stanowi ostatni, najniższy element systemu prawnego. Przyjmuje się zatem zasadę, że każdy pracownik w sytuacji powzięcia przypuszczenia o nieuwzględnieniu w dokumencie aktu prawnego, informuje o tym fakcie przełożonego.

Wykaz załączników.

Załącznik nr 1. Wykaz aktów prawnych.
Załącznik nr 2. Polityka bezpieczeństwa danych osobowych przetwarzanych w zbiorach papierowych.
Załącznik nr 3. Polityka bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych.
Załącznik nr 4. Inwentaryzacja zasobów IT.
Załącznik nr 5. Inwentaryzacja zasobów informacyjnych.
Załącznik nr 6. Wzór umowy powierzenia.
Załącznik nr 7. Ewidencja podmiotów, z którymi została zawarta umowa do przetwarzania danych lub mają dostęp do obszaru przetwarzania danych.
Załącznik nr 8. Obszar przetwarzania danych.
Załącznik nr 9. Ewidencja osób upoważnionych do przetwarzania danych.
Załącznik nr 10. Rejestr czynności przetwarzania.
Załącznik nr 11. Ogólne szacowanie ryzyka.
Załącznik nr 12. Powołanie IOD.
Załącznik nr 13. PIA.
Załącznik nr 14. Wzór rejestru wszystkich kategorii czynności przetwarzania.
Załącznik nr 15. Procedura postpowania w przypadku naruszenia bezpieczeństwa danych.
Załącznik nr 16. Rejestr naruszeń ochrony danych osobowych.
Załącznik nr 17. Upoważnienie dla ASI.
Załącznik nr 18. Upoważnienie do przetwarzania danych.
Załącznik nr 19. Retencja.
Załącznik nr 20. Monitorowanie i sprawdzenie.
Załącznik nr 21. Wyciąg z procedur ochrony danych.
Załącznik nr 22. Szkolenia.
Załącznik nr 23. Aktualizacja i usuwanie danych osobowych.
Załącznik nr 24. Realizacja praw.
Załącznik nr 25. Zarządzanie cyklem życia danych osobowych.
Załącznik nr 26. Niszczenie zbiorów danych osobowych.
Załącznik nr 27. Monitoring Gminny.

Załącznik nr 1. Wykaz aktów prawnych.

1 DANE OSOBOWE PRACOWNIKÓW

- Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 1998 r. Nr 21, poz. 94 z późn. zm.);
- Rozporządzenia Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika (Dz. U. Nr 62, poz. 286 z późn. zm.);
- Ustawa z dnia 30 października 2002 r. o ubezpieczeniu społecznym z tytułu wypadków przy pracy i chorób zawodowych (Dz. U z 2009 r. Nr 167, poz. 1322, z późn. zm.);
- Ustawa z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz.U. z 2013 r. poz. 1440, z późn. zm.);
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.)
- Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 19 grudnia 2002 r. w sprawie trybu uznawania zdarzenia powstałego w okresie ubezpieczenia wypadkowego za wypadek przy pracy, kwalifikacji prawnej zdarzenia, wzoru karty wypadku i terminu jej sporządzenia (Dz.U. z 2013 r. poz.1618 z późn. zm.);
- Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 24 grudnia 2002 r. w sprawie szczegółowych zasad oraz trybu uznawania zdarzenia za wypadek w drodze do pracy lub z pracy, sposobu jego dokumentowania, wzoru karty wypadku w drodze do pracy lub z pracy oraz terminu jej sporządzania (Dz. U. z 2013 r. poz. 924 z późn. zm.);
- Rozporządzenie Rady Ministrów z dnia 1 lipca 2009 r. w sprawie ustalania okoliczności i przyczyn wypadków przy pracy (Dz. U. Nr 105, poz. 870 z późn. zm.);
- Rozporządzenie Ministra Gospodarki i Pracy z dnia 16 września 2004 r. w sprawie wzoru protokołu ustalenia okoliczności i przyczyn wypadku przy pracy (Dz. U. Nr. 227, poz. 2298 z późn. zm.);
- Rozporządzenie Ministra Zdrowia z dnia 1 sierpnia 2002 r. w sprawie sposobu dokumentowania chorób zawodowych i skutków tych chorób (Dz. U. z 2013 r. poz. 1379);
- Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie przekazywania informacji, udostępniania dokumentów oraz udzielania pomocy służbom i instytucjom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego (Dz. U. Nr 258, poz. 1750 z późn. zm.);
- ustawa z 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000).

2 DANE OSOBOWE WYSTĘPUJĄCE PODCZAS REALIZACJI ZADAŃ

- Ustawa z dnia 29 sierpnia 1997 r. Ordynacja podatkowa (Dz. U. z 2012 r. poz. 749 z późn. zm.);
- Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2013 r. poz. 267);
- Ustawa z dnia 10 września 1999 r. Kodeks karny skarbowy (Dz. U. z 2013 r. poz. 186 z późn. zm.);
- Ustawa z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych (Dz. U. z 2012 r. poz. 361 z późn. zm.);
- 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) – RODO;
- Przepisy innych ustaw bezpośrednio związanych z przetwarzaniem danych osobowych w kontekście funkcjonowania organizacji;
- Technika informatyczna – Technika bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji norma ISO/IEC 27001:2014;
- Ustawa z dnia 12 styczeń 1991 r. o podatkach i opłatach lokalnych (Dz. U. z 2017 r., poz.1785 z późn. zm.)
- Ustawa z dnia 15 listopada 1984 r. o podatku rolnym (Dz. U. z 2017 r., poz. 1892 z późn. zm.)
- Ustawa z dnia 30 października 2002 r. o podatku leśnym (Dz. U. z 2017r, poz. 1821 z późn. zm.)
- Ustawa z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz.U. z 2017 r. poz.1201 z późn. zm.)
- Ustawa z dnia 13 września 1996r. o utrzymaniu czystości i porządku w gminach (tj. Dz. U. z 2017r. poz.1289)

Załącznik nr 1. Wykaz aktów prawnych.

- Ustawa z dnia 11 marca 2004r. o podatku od towarów i usług (Dz.U. 2004r Nr 54 poz. 535) - Ustawa z dnia 21.06.2001 r. o ochronie praw lokatorów, mieszkaniowym zasobie gminy i zmianie kodeksu cywilnego (Dz. U.2001r, Nr 71, poz.733)
- Kodeks cywilny z dnia 23.04.1964 r. (Dz. U.1964r, Nr 16, poz. 93)
- Rozporządzenie Ministra Infrastruktury z dnia 14.01.2002 r. w sprawie określenia przeciętnych norm zużycia wody (Dz. U.2002r, Nr 8, poz.70)
- Ordynacja podatkowa (Dz.U.2017r. poz.201)
- Ustawa o Finansach Publicznych (Dz.U. z 2017 r. poz.2077)
- Ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych -(t.j. Dz.U.2017.1464)
- Ustawa z dnia 24 września 2010 r. o ewidencji ludności -(t.j. Dz.U.2017.657)
- Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony - (t.j. Dz.U. z 2017.1430)
- Ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej -(t.j. Dz.U.2018.620)
- Ustawa z dnia 28 listopada 2014 r. Prawo o aktach stanu cywilnego /t.j. Dz.U. z 2016 poz. 2064 z późn. zm./
- ROZPORZĄDZENIE MINISTRA SPRAW WEWNĘTRZNYCH z dnia 9 lutego 2015 r. w sprawie sposobu prowadzenia rejestru stanu cywilnego oraz akt zbiorowych rejestracji stanu cywilnego / t.j. Dz.U.2016.1904/
- Ustawa z dnia 17 października 2008 r. o zmianie imienia i nazwiska /t.j Dz.U. z 2016 poz.10 /
- Ustawa z dnia 25 lutego 1964 r. Kodeks rodzinny i opiekuńczy. /t.j Dz.U. z 2017 poz. 682/
- Ustawa z dnia 21 sierpnia 1997r. o gospodarce nieruchomościami (Dz. U. z 2018 poz. 21);
- Ustawa z dnia 27 marca 2003r. o planowaniu i zagospodarowaniu przestrzennym (Dz. U. z 2017 poz. 1073);
- Ustawa z dnia 7 lipca 1994r. Prawo Budowlane (Dz. U. z 2017 poz. 1332);
- Ustawa z dnia 31 stycznia 1959 r. o cmentarzach i chowaniu zmarłych (Dz. U. z 2017 poz. 912);
- Ustawa z dnia 21 marca 1985 r. o drogach publicznych (Dz. U. z 2017 poz. 2222);
- Ustawa z dnia 28 września 1991 r. o lasach (Dz. U. z 2017 poz. 788);
- Ustawa z dnia 27 kwietnia 2001 r. o odpadach (Dz. U. z 2018 poz. 21);
- Ustawa z dnia 23 lipca 2003 r. o ochronie zabytków i opiece nad zabytkami (Dz. U. z 2017 poz. 2187);
- Ustawa z dnia 16 kwietnia 2004 r. o ochronie przyrody (Dz. U. z 2018 poz. 142);
- Ustawa z dnia 3 lutego 1995 r. o ochronie gruntów rolnych i leśnych (Dz. U. z 2017 poz. 1161);
- Ustawa z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków (Dz. U. z 2017 poz. 2180);
- Ustawa z dnia 4 lutego 1994 r. - Prawo geologiczne i górnicze (Dz. U. z 2017 poz. 2126);
- Ustawa z dnia 27 kwietnia 2001 r. Prawo ochrony środowiska (Dz. U. z 2018 poz. 799);
- Ustawa z dnia 18 lipca 2001 r. Prawo wodne (Dz. U. z 2017 poz. 1121);
- Ustawa z dnia 8 marca 1990 o samorządzie gminnym (Dz. U. z 2017 poz. 1875);
- Ustawa z dnia 3 października 2008 r. o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko;
- Ustawa z dnia 17 maja 1989 r. Prawo geodezyjne i kartograficzne (Dz.U. 2017 poz. 2101);
- Ustawa z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2017 r. poz. 1579);
- Ustawa z dnia 13.10.1995r r. Prawo Łowieckie (Dz.U. z 2017r, poz. 1295 ze zm.)

Załącznik nr 2. Polityka bezpieczeństwa danych osobowych przetwarzanych w zbiorach papierowych.

1. CEL POLITYKI

Celem niniejszego dokumentu jest przedstawienie obowiązujących uregulowań organizacyjno-prawnych, mających bezpośrednie zastosowanie w budowaniu bezpieczeństwa papierowych zbiorów danych. Dokument stanowi opis wdrożonych mechanizmów zapewniających bezpieczeństwo papierowych zbiorów danych, w szczególności prezentuje wprowadzone środki ochrony fizycznej i organizacyjnej. Dokumentacja prowadzona w formie tradycyjnej podlega wielu aktom prawnym m.in. ustawie z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2011 r. Nr 123, poz. 698, z późn. zm.), ustawa z dnia 29 września 1994 roku o rachunkowości (Dz. U .Nr 121, poz. 591 z późn. zm.) i inne, a także dokumenty wewnętrzne. Należy pamiętać o nadrzędnym znaczeniu ustaw i rozporządzeń nad dokumentami wewnętrznymi.

2. ODPOWIEDZIALNOŚĆ

Dokument jest dedykowany wszystkim osobom odpowiedzialnym za prowadzenie papierowych zbiorów danych Urzędu Gminy w Jedwabnie.

3. ZAKRES I WARUNKI STOSOWANIA DOKUMENTU

Niniejszy dokument określa zasady ochrony danych osobowych przetwarzanych w zbiorach papierowych oraz zasady postępowania osób upoważnionych do przetwarzania tych danych.

4. POWIĄZANIA Z INNYMI DOKUMENTAMI

Polityka bezpieczeństwa danych osobowych przetwarzanych w zbiorach papierowych została wyodrębniona jako samodzielny dokument w celu podkreślenia różnic w zastosowanych mechanizmach zabezpieczających, w zależności od sposobu przetwarzania danych.

Dodatkowo, powiązania z innymi uregulowaniami prawnymi, z uwzględnieniem podziału na grupy informacji, zawiera Wykaz aktów prawnych.

5. BEZPIECZEŃSTWO FIZYCZNE I ORGANIZACYJNE

5.1. ŚRODKI FIZYCZNE

W celu zabezpieczenia danych przed nieuprawnionym dostępem, kradzieżą, zmianą, utratą, uszkodzeniem lub zniszczeniem w Urzędzie Gminy w Jedwabnie wykorzystywane są następujące środki fizyczne:

- system alarmowy,
- zamki patentowe,
- szafy zamykane na klucze,
- pomieszczenia zamykane na klucze.

5.2. ŚRODKI ORGANIZACYJNE

W celu zabezpieczenia danych osobowych przed nieuprawnionym dostępem, kradzieżą, zmianą, utratą uszkodzeniem lub zniszczeniem wykorzystywane są następujące środki organizacyjne:

- do prac związanych z dokonywaniem jakichkolwiek operacji na danych dopuszczane są wyłącznie osoby, posiadające imienne upoważnienie do przetwarzania danych osobowych (zgodnie z zakresem czynności wykonywanych na danym stanowisku);
- prowadzona jest *Ewidencja osób upoważnionych do przetwarzania danych osobowych*;
- prowadzone są cykliczne szkolenia dotyczące wymogów ochrony danych osobowych;
- większość zagadnień takich jak: obieg dokumentów, przyjmowanie, otwieranie, sprawdzanie, ewidencjonowane, przydzielanie korespondencji do załatwienia określają zasady, do których postanowień pracownicy winni się stosować.

6. ZASADY PRZETWARZANIA DANYCH

Osoby przetwarzające dane osobowe poza systemem informatycznym muszą zachować następujące zasady podczas ich przetwarzania:

- kategorycznie zabrania się wynoszenia dokumentów zawierających dane osobowe

poza obszar przetwarzania danych, wyjątkiem jest uzyskanie zgody od ADO lub realizacja obowiązków służbowych;

- po przyjściu do pracy pracownik ma obowiązek zwrócić uwagę na stan szaf i zweryfikowanie stanu zabezpieczeń fizycznych;
- w trakcie obecności interesanta na biurku pracownika nie mogą znajdować się żadne dokumenty, które zawierają inne dane osobowe, niż dane przyjmowanej aktualnie osoby;
- po przyjęciu interesanta należy zwrócić uwagę na to, czy nie wynosi on (celowo lub przypadkowo) jakiegokolwiek nie należącego do niego dokumentu;
- podczas przenoszenia dokumentów zawierających dane osobowe należy zachować ostrożność i uwagę, by przypadkowo nie zostawić dokumentu bez opieki (szczególnie dotyczy to kopiowania i drukowania dokumentu);
- po zakończeniu pracy ostatni pracownik opuszczający pomieszczenie zobowiązany jest do sprawdzenia czy szafy są zamknięte oraz zamknięcia pomieszczenia na klucz;
- w Urzędzie Gminy obowiązuje Polityka kluczy.

7. W ZAKRESIE WSZYSTKICH DOKUMENTÓW W FORMIE PAPIEROWEJ OBOWIĄZUJĄ PROCEDURY:

Aktualizacja i usuwanie danych osobowych.

Realizacja praw.

Zarządzanie cyklem życia danych osobowych.

Niszczenie zbiorów danych osobowych.

Załącznik nr 3. Polityka bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych.

Wymogi nakładane na jednostki samorządowe poprzez „Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych" zwarte są w dokumencie System Zarządzania Bezpieczeństwem Informacji.

Realizacja tych zadań realizowana jest poprzez zdefiniowanie zasad zarządzania i wskazanie środków zabezpieczających dla systemów informatycznych przetwarzających dane.

Załącznik nr 4. Inwentaryzacja zasobów IT.

Oprogramowanie komputerowe może być przedmiotem autorskich praw majątkowych lub licencji (zgodnie z ustawą o prawie autorskim i prawach pokrewnych z dnia 4 lutego 1994 r. ze zm.). Zatem oprogramowania nie traktuje się jako rzecz materialną, ale jako wartość niematerialną i prawną. Jednak zarówno nabyte prawo autorskie jak i licencja muszą spełniać wymagania przedstawione w ustawie o rachunkowości (art. 3 ust. 1 pkt 14 ustawy o rachunkowości). Licencje na oprogramowanie są najczęściej bardzo restrykcyjne i większość użytkowników nie czyta ich w ogóle. Większość takich licencji ogranicza liczbę komputerów, na których można zainstalować oprogramowanie, liczbę użytkowników, którzy mogą go używać i wprowadzają wiele innych ograniczeń, które nie są bezpośrednio związane z technologią. Standardowym elementem każdej niemal licencji oprogramowania jest klauzula o wyłączonej odpowiedzialności producenta z tytułu używania oprogramowania przez licencjobiorcę, której znaczenie polega na braku jakiejkolwiek odpowiedzialności producentów oprogramowania za np. skutki błędów w programach. Reakcją na restrykcyjność licencji na oprogramowanie własnościowe są: Licencja GPL i inne licencje FLOSS. Rodzaje licencji które mogą wystąpić to: Abandonware, Adware, AGPL (Affero , blic License), Apache License, APSL (Apple Public Source License), Beerware, BOX, CDDL (Common Development and Distribution License), CPL (Common Public License), Donationware, Freeware, GNU GPL (GNU General Public License), GNU LGPL (GNU Lesser General Public License), IDPL (Initial Developer's Public License), IPL (InterBase Public License), Licencja BSD, Licencja X11 (MIT), MOLP, MPL (Mozilla Public License), NPL (Netscape Public License), OEM (Original Equipment Manufacturer), Postcardware (cardware), Public domain (PD), Shared Source, Shareware, SMSware, Trial, WTFPL. Każdorazowy podczas zakupu czy wdrażania oprogramowania ASI musi zweryfikować rodzaj licencji oraz zachować dowód zakupu (np. kserokopia faktury).

ASI okresowo przeprowadza audyt oprogramowania. Może on być wykonany w sposób tradycyjny lub z wykorzystaniem specjalistycznego oprogramowania. Istotne jest zapoznanie kadry zarządzającej z posiadanym oprogramowaniem.

Poniższe zestawienia urządzeń są przykładowe i wskazują minimalny niezbędny zakres informacji. W przepadku korzystania ze specjalistycznego oprogramowania zasoby sprzętowe powinny być ujawnione kadrze kierowniczej np. w postaci wydruku.

Istotnym elementem inwentaryzacji danych jest dokumentowanie przepływu danych pomiędzy systemami. Dokument taki tworzy ASI i czy to w formie opisu czy w formie grafu ujawnia kadrze kierowniczej.

Dokument może być wytworzony i przechowywany w formie elektronicznej (np. w formacie xls) o ile zawiera minimum dane wskazane w przykładzie.

Komputery lokalne. Stan na dzień: .....

L.p.	Lokalizacja	Urządzenia służące do przetwarzania informacji	Konfiguracja techniczna/ zainstalowane oprogramowanie	Cel, w jakim urządzenie jest wykorzystywane/ wskazanie kategorii danych	Identyfikator użytkownika (osoby której przypisany jest sprzęt)
1.					

Wykaz serwerów. Stan na dzień: .....

L.p.	Lokalizacja	Serwer fizyczny/serwer wirtualny	Konfiguracja techniczna/ zainstalowane oprogramowanie	Cel, w jakim urządzenie jest wykorzystywane/ wskazanie kategorii danych	Uwagi
1.					

Wykaz elementów aktywnych sieci. Stan na dzień: .....

L.p.	Lokalizacja	Nazwa/adres IP urządzenia	Nazwa producenta/ wersja firmware	Uwagi
1.				

Drukarki sieciowe. Stan na dzień: .....

L.p.	Lokalizacja	Druk dwustronny	Właściciel (UG/leasing/...)	Uwagi
1.				

Wykaz użytkowanego oprogramowania. Stan na dzień: .....

L.p.	Lokalizacja fizyczna (zdalny/lokalny)	Producent/dane kontaktowe pomocy technicznej (o ile dostępne)	Uwagi
1.			
2.			

Wykaz posiadanych licencji. Stan na dzień: .....

L.p.	Data uzyskania	Opis oprogramowania/rodzaj licencji	Typ licencji	Numer licencji/ klucza	Identyfikator użytkownika Komputera (osoby której przypisany jest sprzęt)
1.					

Załącznik nr 5. Inwentaryzacja zasobów informacyjnych.

L.p.	*Nazwa*	*Kategoria osób których dane są przetwarzane*	*Określenie kategorii informacji, które są przetwarzane (w maksymalnym możliwym zakresie)*	*Dokumentacja w wersji papierowej*	*Realizacja elektroniczna*	*Opis sposobu przetwarzania*	*Opis celu przetwarzania*	*Podstawa prawna przetwarzania*	*Wskazanie miejsca przechowywania*	*Wskazanie okresu przechowywania*	*Określenie kręgu osób, które mogą mieć dostęp do informacji*	*Właściciel danych*

Załącznik nr 6. Wzór umowy powierzenia do Polityki Bezpieczeństwa.

Przykład 1.

Umowa powierzenia przetwarzania danych osobowych

zawarta dnia ..... pomiędzy:

(zwana dalej „Umową")

.....

*(*dane podmiotu który umowę zawiera)*

zwany w dalszej części umowy **„Podmiotem przetwarzającym"**

reprezentowana przez:

.....

oraz

.....

*(*dane podmiotu który umowę zawiera)*

zwany w dalszej części umowy **„Administratorem danych" lub „Administratorem"**

reprezentowana przez:

.....

§ 1

Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. (zwanego w dalszej części „Rozporządzeniem") dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.

3. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.

§2

Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie umowy dane ..... *(należy podać jak najszerzej rodzaj danych oraz nie stosować itp. itd.)*
   ..... *(należy sprecyzować kategorię osób, których dane dotyczą i doprecyzować zakres tych danych*
2. Powierzone przez Administratora danych dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu .....
   (*cel przetwarzania danych przez podmiot przetwarzający*) *np. realizacji umowy z dnia ..... nr ..... w zakresie prowadzenia kadr.*

§3

Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa/ zwraca Administratorowi wszelkie dane osobowe (*należy doprecyzować oraz określić sposób dokumentowania*)
   oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
6. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.

§4

Prawo kontroli

1. Administrator danych zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum ..... *(należy wpisać z ilu dniowym wyprzedzeniem)* jego uprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż ..... dni (*administrator termin może określić dowolnie*).
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§5

Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora danych.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca, o którym mowa w §3 ust. 2 Umowy winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 6

Odpowiedzialność Podmiotu przetwarzającego

Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Generalnego Inspektora Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

§7

Czas obowiązywania umowy

1. Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas *od* ..... *do* ..... *(lub nieokreślony).*
2. Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem ..... okresu wypowiedzenia.

§8

Rozwiązanie umowy

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

§9

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej.
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

§10

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy dla Administratora danych (*lub Podmiotu przetwarzającego*).

....

Administrator danych *Podmiot przetwarzający*

Przykład 2.

UMOWA

o powierzenie przetwarzania danych osobowych
(dalej: **Umowa**)

zawarta w dniu ..... roku w Jedwabnie pomiędzy:
Gminą Jedwabno z siedzibą ul. Warmińskiej 2, 12-122 Jedwabno, NIP 745-18-11-359
zwanym dalej "Zamawiającym", reprezentowanym przez:
Sławomira Ambroziaka – Wójta Gminy Jedwabno, zwanym dalej Zleceniodawcą:
a
.....
.....
zwaną dalej "Wykonawcą",
zwanymi łącznie dalej **Stronami**

Zważywszy, że:

1) Strony łączy umowa z dnia ..... o realizacji zamówienia na .....
(dalej: **Umowa Główna**);
2) Zleceniodawca przekazuje Wykonawcy dane osobowe w celu wykonywania Umowy Głównej,

Strony postanawiają zawrzeć Umowę o następującej treści:

§ 1

1. Zleceniodawca powierza Wykonawcy przetwarzanie danych osobowych w celu wykonywania Umowy Głównej, co stanowi udokumentowane polecenie przetwarzania w rozumieniu art. 29 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), dalej: RODO.
2. Wykonawca jest uprawniony do przetwarzania przekazanych danych osobowych wyłącznie w zakresie oraz w celu zgodnym z niniejszą Umową.
3. Wykonawca może przetwarzać następujące dane osobowe: .....
4. Przetwarzanie danych przez Wykonawcę trwa do chwili rozwiązania, wygaśnięcia lub zakończenia Umowy, chyba że Wykonawca wcześniej usunie ww. dane osobowe na wniosek Zamawiającego.

§ 2

1. Zleceniodawca oświadcza, iż jest administratorem danych osobowych powierzonych Wykonawcy.
2. Wykonawca oświadcza, że jest podmiotem przetwarzającym dane osobowe na zlecenie Zleceniodawcy zgodnie z niniejszą Umową.
3. Wykonawca oświadcza, że:
    a. posiada środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych osobowych w zakresie wymaganym przez obowiązujące Wykonawcę przepisy prawa, a w szczególności zabezpiecza dane osobowe przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem tych danych, a także spełnia inne wymagania określone w przepisach prawa dotyczące ochrony danych osobowych;

   b. prowadzi wymaganą przepisami prawa dokumentację opisującą sposób przetwarzania danych osobowych.
4. Wykonywanie Umowy nie wiąże się z żadnymi świadczeniami pieniężnymi ze strony Zleceniodawcy, a wszelkie rozliczenia finansowe dokonane zostaną w ramach Umowy Głównej.
5. Wykonawca zobowiązuje się, że:
   a. będzie prowadził ewidencję osób upoważnionych (ze strony Wykonawcy), zgodnie z przepisami prawa;
   b. zachowa w tajemnicy dane osobowe oraz inne dane, a w szczególności informacje stanowiące tajemnicę przedsiębiorstwa, do których Wykonawca mógł uzyskać dostęp w związku z wykonywaniem Umowy lub Umowy Głównej, także po wygaśnięciu lub rozwiązaniu Umowy Głównej;
   c. zobowiąże na piśmie pracowników oraz inne osoby współpracujące na podstawie umów cywilno-prawnych z Wykonawcą, posiadające lub mogące posiadać dostęp do danych udostępnionych przez Zleceniodawcę w związku z wykonywaniem Umowy Głównej do ich zachowania w tajemnicy również po ustaniu stosunku pracy lub innego stosunku cywilnoprawnego łączącego dany podmiot z Wykonawcą;
   d. przy wykonywaniu Umowy dołoży staranności, wynikającej z profesjonalnego charakteru wykonywanej działalności;
   e. niezwłocznie poinformuje Zleceniodawcę o każdym przypadku naruszenia bezpieczeństwa jakichkolwiek informacji udostępnionych Wykonawcy przez Zleceniodawcę w związku lub w trakcie wykonywania Umowy Głównej, w tym w szczególności w przypadku naruszenia zasad ochrony danych osobowych;
   f. poinformuje Zleceniodawcę o każdym przypadku naruszenia zobowiązań wynikających z Umowy niezwłocznie, nie później niż w terminie 2 dni od chwili stwierdzenia naruszenia;
   g. podejmuje wszelkie środki wymagane na mocy art. 32 RODO;
   h. przetwarza dane osobowe zgodnie z Umową Główną (udokumentowane polecenie Zleceniodawcy) – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega Wykonawca; w takim przypadku przed rozpoczęciem przetwarzania Wykonawca informuje Zleceniodawcę o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny,
   i. w miarę możliwości będzie pomagać Zleceniodawcy - poprzez odpowiednie środki techniczne i organizacyjne - wywiązać się z obowiązku odpowiadania na żądania osoby, której dane osobowe dotyczą, w zakresie wykonywania praw tej osoby określonych w art. 32-36 RODO – realizowane jest to bez dodatkowych opłat;
   j. uwzględniając charakter przetwarzania danych osobowych oraz dostępne informacje Wykonawca - wyłącznie w zakresie związanym z wykonywaniem Umowy Głównej - w miarę możliwości pomaga Zleceniodawcy poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w Rozdziale III RODO- realizowane jest to bez dodatkowych opłat;
   k. wyłącznie w zakresie związanym z wykonywaniem Umowy Głównej udostępni Zleceniodawcy wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO przez Wykonawcę.
6. Po rozwiązaniu Umowy Głównej Wykonawca – według wyboru Zleceniodawcy w formie pisemnej pod rygorem nieważności - wyda Zleceniodawcy lub usunie w sposób trwały wszystkie dane osobowe pochodzące od Zleceniodawcy lub wytworzone na polecenie Zleceniodawcy. W braku decyzji Zleceniodawcy przyjmuje się, że Zleceniodawca wydaje

polecenie zwrotnego wydania wszystkich materiałów zawierających dane osobowe do rąk własnych.

§ 3

1. Wykonawca oświadcza, że przy przetwarzaniu danych nie będzie korzystać z usług podmiotów trzecich i dane osobowe nie będą przekazywane poza terytorium Unii Europejskiej.
2. Wykonawca może powierzyć przetwarzanie przekazanych danych osobowych podmiotom trzecim wyłącznie za uprzednią, pisemną zgodą Zleceniodawcy.

§ 4

1. Zleceniodawca ma prawo do kontroli zgodności przetwarzania danych osobowych przez Wykonawcę z przepisami prawa lub Umową, w tym jest uprawniony do żądania od Wykonawcy udzielenia informacji dotyczących wywiązania się z zobowiązań, o których mowa w Umowie oraz do żądania usunięcia uchybień w tym zakresie w odpowiednim terminie wskazanym przez Zleceniodawcę, nie dłuższym jednak niż 7 dni roboczych od dnia wystąpienia przez Zleceniodawcę z żądaniem w tym zakresie.
2. Zleceniodawca ma prawo przeprowadzić audyt lub inspekcję w siedzibie lub innym miejscu, gdzie przetwarzane są dane osobowe przez Wykonawcę za 7-dniowym uprzedzeniem. Audyt, o którym mowa w zdaniu pierwszym, jest przeprowadzany na koszt Zleceniodawcy. Zleceniodawca zobowiązuje się przeprowadzić audyt w taki sposób, aby zminimalizować ryzyko zakłócenia pracy Wykonawcy oraz zachować w tajemnicy wszelkie informacje poufne, w tym stanowiące tajemnicę przedsiębiorstwa.

§ 5

1. Umowa zostaje wchodzi w życie z dniem ..... roku i zostaje zawarta na czas nieokreślony z zastrzeżeniem ust. 2.
2. Umowa wygasa z chwilą wygaśnięcia, rozwiązania lub zakończenia w inny sposób Umowy Głównej.
3. Zleceniodawca ma prawo wypowiedzenia Umowy Głównej oraz Umowy ze skutkiem natychmiastowym w przypadku, gdy Wykonawca naruszy którykolwiek z obowiązków określonych w § 2 lub § 3 Umowy lub Wykonawca nie zastosuje się do żądania Zleceniodawcy lub nie usunie uchybień zgodnie z § 4 ust. 1 i 2 Umowy.
4. Zmiany niniejszej Umowy mogą zostać dokonane w formie pisemnej pod rygorem nieważności.
5. Jeżeli jakiekolwiek postanowienia Umowy okażą się nieważne nie uchybia to mocy pozostałym, a Strony będą dążyć do zastąpienia nieważnego postanowienia ważnym zapisem odzwierciedlającym pierwotną wolę Stron.
6. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

.....	.....
Zleceniodawca	*Wykonawca*

Załącznik nr 7. Ewidencja podmiotów, z którymi została zawarta umowa do przetwarzania danych lub mają dostęp do obszaru przetwarzania danych.

Dane firmy z którą zawarto umowę, data zawarcia	Osoba do kontaktu (imię, nazwisko, numer telefonu)	Zakres wykonywanego zobowiązania	Uwagi (np. zakończenie umowy)

WYKAZ OBSZARÓW PRZETWARZANIA

danych osobowych i innych informacji chronionych w Urzędzie Gminy w Jedwabnie .

Lp.	Adres	nr pokoju lub/i nazwa działu/pomieszczenia

.....

data aktualizacji

.....

podpis IOD

Ewidencja osób upoważnionych do przetwarzania danych osobowych.

Nr	Imię i nazwisko osoby upoważnionej	Data nadania upoważnienia	Data ustania upoważnienia (jeśli inna niż spowodowana czynnikami „naturalnymi" (wygaśnięcie umowy o pracę, wygaśnięcie mandatu)	Uwagi
1.				
2.				
3.				
4.				
5.				

ości przetwarzania.

Jednostka organizacyjna partament, dział itp.)	Cel przetwarzania	Kategorie osób	Kategorie danych	Planowany termin usunięcia kategorii danych (jeżeli jest to możliwe)	Kategorie odbiorców (innych niż podmiot przetwarzajacy)	Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)	Podstawa prawna	Źródło danych	Naz opro

PCL XL error

Warning: IllegalMediaSize

Szacowanie Ryzyka (Metodologia)

Ogólne szacownie ryzyka można przeprowadzić wieloma metodami i z wykorzystaniem różnorodnych narzędzi.

Polityka nie wskazuję jednoznacznej metody analizy ryzyka, którą należy się posługiwać. Niemniej jednak biorąc pod uwagę zapisy normy ISO/IEC 27001, która odwołuje się do dokumentu ISO/IEC TR 13335-3 do możliwych do użycia metodyk należą:

- AS/NZS 4360:2004 metodologia opublikowana przez Australia Standards i New Zealand Standards;
- COBRA (Control Objectives for Risk Analysis);
- CRAMM – „CCTA Risk Assessment and Management Methodology" metodyka pierwotnie opracowana na potrzeby rządu Wielkiej Brytanii;
- CiticusOne – bazująca na jednej z najbardziej znanych metodyk analizy ryzyka zwanej FIRM, opracowanej przez Information Security Forum;
- FMEA (Failure Mode and Effect Analysis);
- ISO 31000 – nowy standard ISO, zawierający wytyczne w zakresie ogólnego implementowania procesu zarządzania ryzykiem.
- Mehari – metoda zarządzania i analizy ryzyka rozwijana przez Club de la Sécurité de l'Information Francis;
- OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation).

Zapisy normy przewidują także „metody własne", które mogą zostać wypracowane przez konkretną organizację np. na postawie wiedzy branżowej czy zgromadzonego doświadczenia. Niewątpliwą korzyścią zastosowania takiej metody jest jej **pełna świadomość**, jak również całego procesu szacowania ryzyka przez wszystkich uczestników biorących udział przy jej wykorzystaniu w procesie szacowania ryzyka bezpieczeństwa informacji.

Poniżej przedstawiono jeden z możliwych sposobów wykonania analizy ryzyka.

1. Należy wskazać, w stosunku do czego przeprowadza się szacowanie ryzyka, z uwzględnieniem wyników przeprowadzonej inwentaryzacji oraz należy objąć nim cały „cykl życia" informacji – od jej wpłynięcia lub wygenerowania, do zarchiwizowania lub usunięcia.
2. Przed przystąpieniem do szacowania należy ustalić osobę bezpośrednio odpowiedzialną za rozpatrywany zasób informacyjny.
3. Należy ustalić wartość zasobu informacyjnego (np. w skali od 1 do 4), w zależności od rodzaju i znaczenia informacji w nim zawartych - czy są tam informacje o stanie zdrowia, wysokości wynagrodzenia, czy jedynie o adresie zamieszkania i wykształceniu. Jak na poniższej tabeli:

Wartość zasobu	Kategorie informacji
(4) **Wrażliwe**	**Wyłącznie: dane dotyczących zdrowia, pochodzenia rasowego, etnicznego, poglądów politycznych, przekonań religijnych, światopoglądowych, przynależności do związków zawodowych, dane genetyczne, dane biometryczne (w celu identyfikacji), dane dotyczące seksualności, orientacji seksualnej**
(3) **Finansowe**	**Np. wysokość wynagrodzenia, historia operacji finansowych, dokumenty związane z korzystaniem z usług bankowości, inwestycje, katy kredytowe, faktury, dokumenty ubezpieczeniowe odnoszące się do statusu materialnego**
(2) **Behawioralne** (świadczące o zachowaniu)	**Np. zwykła historia przeglądania stron internetowych, informacje o lokalizacji (np. z aplikacji do nawigacji), informacje o ruchu sieciowym (bilingi, numer ip), informacje o osobistych nawykach i zwyczajach**
(1) **Proste**	**Np. Imię nazwisko, doświadczenie zawodowe, kwalifikacje, wykształcenie, dane kontaktowe (adres mail, nr telefonu)**

4. Po ustaleniu kontekstu rozpatrujemy scenariusze możliwych zagrożeń, których lista została zawarta poniżej.
5. Jeżeli w odniesieniu do naszej działalności potrafimy wskazać inne, nieprzewidziane we wzorze scenariusze zagrożeń – należy je dopisać.

6. Przy rozpatrywaniu scenariuszy musimy wziąć pod uwagę **„aktywa wspierające”**, czyli narzędzia, lokalizacje, ludzi bezpośrednio wykorzystujących np. konkretne dokumenty lub programy, dla których przeprowadzane jest szacowanie.
7. Przy rozpatrywaniu scenariuszy uwzględniamy też **obecnie stosowane** (na moment szacowania ryzyka) zabezpieczenia przed realizacją konkretnego scenariusza.
8. To przede wszystkim od tego, jakie **„podatności”** posiadają „aktywa wspierające” zależy ustalenie **„prawdopodobieństwa”** realizacji konkretnego scenariusza.
9. Np. szafa drewniana jest bardziej podatna na spalenie w wyniku pożaru niż szafa metalowa, pomieszczenie na parterze jest bardziej podatne na włamanie niż pomieszczenie na piętrze, praca w warunkach podróży służbowych oznacza większą podatność na zagubienie dokumentów lub sprzętu niż praca w trybie stacjonarnym, starsza wersja systemu operacyjnego jest bardzie podatna na złośliwe oprogramowanie niż nowsza.
10. Należy ustalić, jakie może być ich źródło zagrożeń np. własny pracownik, klient, złodziej, włamywacz, haker, czynniki klimatyczne itd.
11. Poprzez rozpatrywanie scenariuszy staramy się odpowiedzieć na pytanie, co może spowodować (co może być źródłem oraz poprzez jakie podatności może się to zrealizować): -utraty **dostępności**, **poufności**, **integralności**
12. Dotkliwość naruszenia będzie pochodną ustalenia wartości zasobu, ale będzie ona zależała także od kontekstu rozpatrywanego scenariusza np. od intencji sprawcy, źródła zagrożenia, długości trwania skutku, przewidywanego praktycznego wpływu na sytuację osoby fizycznej. Przy ocenie dotkliwości należy kierować się wskazaniami zawartymi w macierzy ryzyka.
13. Dotkliwość naruszenia musimy oceniać **z perspektywy osoby, której potencjalne naruszenie może dotyczyć**, inaczej mówiąc, musimy postarać się odpowiedzieć na pytanie, **co złego mogłoby się stać osobie, której danych dotyczyłby konkretny scenariusz,** z jakimi trudnościami spotkałaby się ta osoba.
14. Poziom ryzyka określamy w ramach skali przedstawionej na macierzy ryzyka (NISKIE, ŚREDNIE, PODWYŻSZONE, WYSOKIE).
15. Poziom ryzyka wynika z kombinacji stwierdzonego **prawdopodobieństwa** ze stwierdzonym stopniem **dotkliwości** (jak na poniższej macierzy ryzyka).

MACIERZ RYZYKA						
PRAWDOPODOBIEŃSTWO		**DOTKLIWOŚĆ***				
		1 (MINIMALNA) Osoby w żadnym stopniu nie odczują negatywnych następstw.	**2 (UMIARKOWANA)** Osoby mogą napotkać kilka niedogodności, które pokonają bez problemu (czas poświęcony na	**3 (ŚREDNIA)** Osoby mogą napotkać zauważalne niedogodności,	**4 (ZNACZNA)** Osoby mogą napotkać znaczące konsekwencje, które powinny być	**5 (KRYTYCZNA)** Osoby mogą napotkać znaczne, a nawet nieodwracalne konsekwencje,

			ponowne wprowadzanie informacji, chwilowe rozdrażnienie, poirytowanie itp.).	które będą w stanie przezwyciężyć pomimo kilku trudności (dodatkowe koszty, odmowa dostępu do usług biznesowych, strach, brak zrozumienia, stres, niewielkie dolegliwości fizyczne itd.)	w stanie przezwyciężyć, choć z poważnymi trudnościami (sprzeniewierzenie funduszy, utrata wiarygodności kredytowej, szkody materialne, utrata zatrudnienia, wezwanie do sądu, pogorszenie stanu zdrowia itp.).	których mogą nie przezwyciężyć (trudności finansowe, takie jak znaczny dług lub brak możliwości zatrudnienia, długoterminowe dolegliwości psychologiczne lub fizyczne, śmierć itp.).
	5 (PEWNE) Zdarzenie jest praktycznie możliwe i wiemy, że dojdzie do jego zajścia (jest nieuniknione w krótszej, lub dłuższej perspektywie czasowej).	Ś	P	W	W	W
	4 (PRAWIE PEWNE) Zdarzenie jest praktycznie możliwe, spodziewamy się jego zajścia (w krótszej lub dłuższej perspektywie czasowej), ale można go uniknąć.	Ś	P	P	W	W
	3 (MOŻLIWE) Zdarzenie jest praktycznie możliwe (można się spodziewać jego zajścia w krótszej, lub dłuższej perspektywie czasowej), ale wyżej oceniamy szansę na brak zajścia zdarzenia.	N	Ś	P	P	W

	2 (ZNIKOME) Zdarzenie jest teoretycznie możliwe, ale jego spełnienie wymagałoby okoliczności, które nigdy w przeszłości nie zaszły, lecz nie można wykluczyć ich zajścia w przyszłości, choć byłoby to niespodziewane	N	N	Ś	Ś	P
	1 (NIEREALNE) Zdarzenie jest teoretycznie możliwe, ale jego spełnienie wymagałoby okoliczności, które nigdy w przeszłości nie zaszły, i - oceniając z praktycznego punktu widzenia- nie zajdą	N	N	N	N	Ś
W – Wysoki poziom ryzyka; P – Podwyższony poziom ryzyka; Ś – Średni poziom ryzyka; N – Niski poziom ryzyka						

16. Po zidentyfikowaniu podatności aktywów wpierających, źródeł ryzyka oraz stwierdzeniu istniejącego poziomu ryzyka – możemy je zaakceptować, jeżeli jest NISKIE tzn. nie ma powodu by stosować nowe, dodatkowe zabezpieczenia. Jest to pożądany do osiągnięcia, docelowy poziom ryzyka.
17. W przypadku stwierdzenia WYSOKIEGO poziomu ryzyka w odniesieniu do konkretnego scenariusza, należy priorytetowo odpowiedzieć na pytanie– jakie dodatkowe zabezpieczenia mogą wpłynąć na zredukowanie poziomu ryzyka, w większości przypadków zredukowanie poziomu ryzyka można osiągnąć poprzez zastosowanie nowych, dodatkowych zabezpieczeń, które eliminują podatności (np. wymiana szafy z drewnianej na metalową, aktualizacja systemu operacyjnego, wprowadzenie zasady szyfrowania niektórych dysków przenośnych itd.) wpływające na zmniejszenie prawdopodobieństwa realizacji scenariusza.
18. W przypadku stwierdzenia PODWYŻSZONEGO poziomu ryzyka, należy także sformułować listę dodatkowych zabezpieczeń, które mogłyby wpłynąć na redukcję poziomu ryzyka, różnica polega na tym, że w planie postępowania z ryzykiem, opisanym w protokole

szacowania ryzyka należy w pierwszej kolejności wprowadzić te zabezpieczenia, które zredukują WYSOKIE ryzyko (tzn. w pierwszej kolejności wydajemy budżet na te zabezpieczenia, które zredukują WYSOKIE ryzyko, a nie PODWYŻSZONE).

19. W przypadku stwierdzenia ŚREDNIEGO poziomu ryzyka, możliwe jest jego zaakceptowanie, rekomendowane jest jednak by sformułować listę dodatkowych zabezpieczeń redukujących poziom ryzyka, które zostaną wprowadzone, o ile będzie to możliwe i zostaną wygospodarowane środki. W przypadku jego akceptacji należy pilnie monitorować, czy nie powoduje do dalszych negatywnych następstw w praktyce.
20. Efektem szacowania ryzyka będzie protokół szacowania ryzyka, który powinien zawierać określenie stwierdzonych poziomów ryzyka dla konkretnego zasobu (pomocniczo można wykorzystać **przykładowo uzupełniony protokół)**, oraz zawarty w pkt 4 plan postępowania z ryzykiem, zawierający opis decyzji co do zredukowania wskazanych poziomów ryzyka (do NISKIEGO lub ŚREDNIEO), oraz wybór środków, którymi ten cel zostanie osiągnięty.
21. W ramach planu postępowania z ryzykiem należy wskazać, jakie podatności zostaną wyeliminowane lub ograniczone przez wprowadzane zabezpieczenie oraz określić czas w perspektywie nowe zabezpieczeni zostanie wdrożone.
22. Domyślnie przyjmuje się, że osoba sporządzająca protokół szacowania ryzyka jest odpowiedzialna z wdrożenie zabezpieczeń wskazanych w planie postępowania z ryzykiem, może to być inna osoba, ale należy wyraźnie zadbać o świadomość tego obowiązku.
23. Szacowanie ryzyka powinno być przeprowadzone dla wszystkich sposobów, operacji lub czynności przetwarzania, tak istniejących, jak i tych, które zostaną wprowadzone w przyszłości.
24. Oszacowane ryzyka powinny zostać poddawane okresowym przeglądom nie rzadszym niż raz na rok, a przypadku zmian okoliczności mogących mieć wpływ na stwierdzone poziomy ryzyka, szacowanie należy powtórzyć.
25. W przypadku wykonywania kolejnych przeglądów ryzyka lub wykonywania nowego szacowania ryzyka, przy ustalaniu prawdopodobieństwa realizacji scenariuszy należy uwzględnić incydenty i zdarzenia, które miały miejsce pomiędzy poszczególnymi przeglądami lub szacowaniami ryzyka.
26. W przypadku ustalenia, że prowadzone są operacje przetwarzania związane z obowiązkiem sporządzenia szczegółowego raportu zawierającego ocenę skutków dla ochrony danych w rozumieniu art. 35 RODO– czyli operacje przetwarzania, które wiążą się z **dużym prawdopodobieństwem** możliwości powodowania **wysokiego ryzyka** naruszenia praw lub wolności osób fizycznych (dla tych operacji konieczne będzie sporządzenie dodatkowego raportu, najlepiej zgodnie z normą ISO 29134). Dotyczyć to będzie tych operacji przetwarzania, dla których po przeprowadzeniu ogólnego szacowania ryzyka i wprowadzeniu planu postępowania z ryzykiem, nie uda się zredukować wysokiego ryzyka (lub tych, które znajdą się na liście operacji przetwarzania wydanej przez organ nadzorczy – Prezesa UODO).

Scenariusze dla dokumentów tradycyjnych.

Nazwa zasobu: ..... Wartość zasobu .... Osoba odpowiedzialna: .....)						
Dostęp do treści dokumentów papierowych zawierających dane osobowe **uzyska osoba do tego nieuprawniona** (należy zwrócić uwagę na możliwość zabrania dokumentu lub jego modyfikacji):	Podatności	Źródła ryzyka	Istniejące zabezpieczenia	Prawdopodobieństwo	Określenie stwierdzonego poziomu ryzyka w oparciu o macierz ryzyka z załącznika nr 7, opis skutków dla osób, których dane są przetwarzane	Zalecenia i wpływ ich realizacji na modyfikację poziomu ryzyka
a) firma sprzątająca (sprzątaczka)						
b) pracownik z innego działu lub stanowiska, który nie ma prawa dostępu do konkretnych dokumentów						
c) klient						
d) złodziej/włamywacz (także utrata dostępności)						
e) inna osoba (*np. przy zabieraniu dokumentów do domu lub poprzez niedostateczne zniszczenie papierowego*						

dokumentu)						
f) poprzez spalenie *(np. w wyniku pożaru)*						
g) poprzez zalanie						
h) poprzez wywianie przez otwarte okno						
i) poprzez zgubienie						
j) poprzez omyłkowe wrzucenie dokumentu do niszczarki						
k) poprzez omyłkowe wrzucenie dokumentu do kosza na śmieci (*dodatkowo możliwość zapoznania się z treścią przez osoby nieuprawnione*)						
l) zgubienie klucza do mebli zamykanych w których przechowywane są dokumenty						
m) Zgubienie klucza do pomieszczenia w którym przechowywane są dokumenty						

Scenariusz dla dokumentów elektronicznych.

Nazwa zasobu: ..... Wartość zasobu .... Osoba odpowiedzialna:						
Osoba nieuprawniona uzyskuje dostęp do treści dla niej nieprzeznaczonej	Podatności	Źródła ryzyka	Istniejące zabezpieczenia	Prawdopodobieństwo	Określenie stwierdzonego poziomu ryzyka w oparciu o macierz ryzyka z załącznika nr 7, opis skutków dla osób, których dane są przetwarzane	Zalecenia i wpływ ich realizacji na modyfikację poziomu ryzyka
a) poprzez zaglądanie do ekranu „przez ramię" (odmienne prawdopodobieństwo przy sprzęcie stacjonarnym, odmienne przy sprzęcie mobilnym np. w hotelu, pociągu, podróży służbowej itd.)						
b) poprzez uzyskanie hasła dostępowego						
c) poprzez złamanie hasła dostępowego						
d) Poprzez włamanie się na urządzenie korzystające z otwartej sieci wifi						
e) Poprzez włamanie się na urządzenie						

korzystające z komunikacji bezprzewodowej np. poprzez bluetooth						
f) Poprzez zainstalowanie złośliwego oprogramowania (trojany, keyloggery, wirusy						
g) poprzez dostęp do urządzenia, które nie jest zabezpieczone hasłem						
h) poprzez omyłkowe wysłanie maila na błędny adres						
i) poprzez przechwycenie komunikacji elektronicznej						
j) poprzez przekupienie pracownika posiadającego dostęp do danych (skopiowanie danych i przeniesienie na zewnątrz)						
k) w efekcie utraty zasilania						
l) w efekcie awarii komputera (np. uszkodzony dysk twardy wyładowanie na linii energetycznej)						
m) w efekcie utraty						

danych dostępowych (hasło)						
n) w efekcie zaszyfrowania komputera oprogramowaniem złośliwym typu ransomware						
o) w efekcie omyłkowego wykasowania dokumentu						
p) w efekcie kradzieży sprzętu (odmienne prawdopodobieństwo przy sprzęcie stacjonarnym, a odmienne przy sprzęcie mobilnym np. w hotelu, pociągu, samochodzie itd.)						
q) w efekcie zniszczenia sprzętu poprzez zalanie						
r) w efekcie zniszczenia sprzętu poprzez pożar						
s) w efekcie zagubienia urządzenia mobilnego (smartfon/laptop/tablet) Dodatkowo – ryzyko naruszenia poufności zgromadzonych informacji						
t) w efekcie zagubienia nośnika informacji (pendrive, dysk						

przenośny, płyta cd/dvd itd.) Dodatkowo – ryzyko naruszenia poufności zgromadzonych informacji						

Inspektor Ochrony Danych ma prawo wykorzystać inną metodę, szczególnie jeśli wykorzystuje ona większą niż wykazana ilość czynników. Forma może być elektroniczna lub papierowa. Dla zachowania ciągłości oceny, wskazanie jest wykorzystywanie jednej metody, a w przypadku jej zmiany, badanie w którym rozpoczynamy czynność oceny inna metodą musi być uzupełnione o badanie metodą zmienianą. Z badania sporządza się protokół uwzględniający zarówno rejestr występującego ryzyka jak i sposób z nim postępowania.

Załącznik 12. Powołanie IOD.

Jedwabno, dn. .....

POWOŁANIE

funkcji Inspektora Ochrony Danych w .....

Na art. 37 ust. 1 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, zwane dalej RODO, powołuję Pana:

.....

na funkcję Inspektora Ochrony Danych

Na podstawie art. 39 RODO, powierzam Pani/Panu zadania związane z utrzymaniem bezpieczeństwa informacji, a w szczególności:

Lp.	zadanie	termin wykonania
1.	informowanie administratora, podmiot przetwarzający oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich z mocy RODO oraz innych przepisów krajowych w zakresie ochrony danych osobowych	wg. potrzeb
2.	monitorowanie przestrzegania RODO, innych przepisów krajowych dot. ochrony danych osobowych oraz polityk Administratora	wg. potrzeb
3.	przedstawianie harmonogramu czynności audytowych zgodnie z przyjętą Polityką Bezpieczeństwa Informacji (PBI)	do końca grudnia na rok kolejny
4.	przeprowadzanie czynności audytowych zgodnie z przedstawionym wcześniej harmonogramem	minimum raz w roku
5.	udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych osobowych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO	wg. potrzeb
6.	współpraca z organem nadzorczym	wg. potrzeb
7.	pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszystkich innych sprawach	wg. potrzeb
8.	opiniowanie wprowadzonych przez Administratora polityk, procedur, analiz oraz rejestrów czynności	wg. potrzeb

Informuję Panią/Pana, iż w ramach powierzonych obowiązków jest Pani/Pan uprawniona do:

1. wstępu do pomieszczeń, w których przetwarzane są dane osobowe,
2. odbierania wyjaśnień od osób przetwarzających dane osobowe,
3. dokumentowania ustaleń i dokonywania innych czynności niezbędnych do wykonania zadań wynikających niniejszego upoważnienia.

OŚWIADCZENIE INSPEKTORA OCHRONY DANYCH

Oświadczam, iż będę wypełniać swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania danych w ... .
Niniejszym zobowiązuję się do zachowania poufności, nieujawniania osobom nieupoważnionym i zachowania w tajemnicy wszelkich danych z którymi mam styczność podczas wykonywania powierzonych mi zadań, a dane te nie są danymi publicznymi.
Potwierdzam, że zapoznałem się z Polityką Bezpieczeństwa Informacji oraz wszelkimi regulacjami i procedurami z tego zakresu, wprowadzonymi przez Administratora Danych.
Oświadczam, iż spełniam wymogi art. 37 ust. 5 i 6 RODO, oraz wyrażam zgodę na upublicznienie mojego imienia i nazwiska oraz danej kontaktowej w postaci adresu e-mail w celu dokonania obowiązku określonego w art. 37 ust. 7 RODO.

....

data i podpis IOD podpis ADO

Ocena skutków ochrony danych.

Preferowanym narzędziem ceny skutków dla ochrony danych jest opracowane przez francuski organ ochrony danych osobowych narzędzie PIA. Jest ono dostępne na stronie tego organu (https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment) w kilku wersjach językowych. Polskie tłumaczenie zaproponowane przez niezależną osobę, zostało doprecyzowane i zatwierdzone przez polski organ nadzorczy. Ułatwia ono przeprowadzenie oceny skutków ochrony danych, która jest obowiązkowa w przypadku operacji przetwarzania danych określonych m.in. w paragrafie 9 i 10 RODO.
IOD może stosować inne metody oceny bezpieczeństwa, w tym kompleksowe.

Załącznik nr 14. Wzór rejestru wszystkich kategorii czynności przetwarzania.

*Kolorem czerwonym oznaczono informacje wymagane w rejestrze przez art. 30 ust. 2 RODO

	1	2	3	4	5	6	7	8	9	10	11	12
LP.	Kategorie przetwarzań	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe)	Administrator				Czas trwania przetwarzania (data końca)	Data modyfikacji, powód modyfikacji, podpis	Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane	Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi	Podprzetwarzający (podwykonawca) - jeśli	
			Nazwa i dane kontaktowe administratora	Nazwa i dane kontaktowe współadministratora (jeśli dotyczy)	Nazwa i dane kontaktowe przedstawiciela administratora (jeśli wyznaczono)	Inspektor ochrony danych administratora (jeśli powołano)					Nazwa i dane kontaktowe podprzetwarzającego (podwykonawcy)	Kategorie podpowierzonych przetwarzań
	Art. 30 ust. 2 lit. b	Art. 30 ust. 2 lit. d, art. 32 ust. 1	Art. 30 ust. 2 lit. a						Art. 30 ust. 2 lit. c	Art. 30 ust. 2 lit. c		
1												
2												
3												
4												
5												
6												
7												
8												
9												
10												

Procedura postępowania w przypadku naruszenia bezpieczeństwa danych.

1. Wszelkie osoby, które mają styczność z danymi osobowymi powinny być uświadomione o potencjalnych, najbardziej prawdopodobnych naruszeniach ochrony danych osobowych właściwych dla swojego obszaru działania oraz zobowiązane do niezwłocznego powiadamiania o potencjalnych naruszeniach bezpośredniego przełożonego – minimalnym rozwiązaniem jest przedłożenie do zapoznania się dostosowanego do sytuacji przedsiębiorstwa załącznika ***Wyciąg z procedur ochrony danych***.
2. Niezależnie od posłużenia się treścią załącznika ***Wyciąg z procedur ochrony danych***, przynajmniej raz w roku, należy dokonać przeglądu scenariuszy zawartych z załączniku ***Ogólne szacowanie ryzyka*** w formie dyskusji ze wszystkimi osobami upoważnionymi do przetwarzania lub reprezentantami poszczególnych działów.
3. Z dyskusji sporządza się notatkę, która powinna uwzględniać ustalone wnioski co do uwzględnienia nowych scenariuszy zagrożeń – lub braku konieczności modyfikacji dotychczas rozpatrywanych scenariuszy zagrożeń.
4. Po powzięciu informacji o potencjalnym naruszeniu ochrony danych osobowych, należy niezwłocznie zbadać okoliczności zgłaszanego zdarzenia.
5. Badanie okoliczności zdarzenia nie może zostać ukończone później niż w ciągu 24 godzin od powzięcia informacji o potencjalnym naruszeniu
6. W przypadku zdarzeń, które wymagają dłuższej analizy do stwierdzenia lub wykluczenia naruszenia należy przygotować pisemne uzasadnienie konieczności dłuższego badania.
7. Po zbadaniu naruszenia należy uzupełnić część pierwszą protokołu naruszenia, stanowiącą załącznik nr 1 do bieżącego dokumentu, podając wszystkie wymagane w niej informacje.
8. W przypadku potwierdzenia, że do naruszenia ochrony danych osobowych doszło, należy niezwłocznie przystąpić do uzupełnienia części drugiej protokołu, z uwzględnieniem kroków wskazanych w pkt 9-18:
9. Należy ustalić jakich kategorii danych osobowych dotyczyło stwierdzone naruszenie, dokonując wyboru jednej z 4 kategorii wskazanych w tabeli poniżej:

Wartość zasobu	Kategorie informacji
(4) **Wrażliwe**	**Wyłącznie: dane dotyczących zdrowia, pochodzenia rasowego, etnicznego, poglądów politycznych, przekonań religijnych, światopoglądowych, przynależności do związków zawodowych, dane genetyczne, dane biometryczne (w celu identyfikacji), dane dotyczące seksualności, orientacji seksualnej**
(3) **Finansowe**	**Np. wysokość wynagrodzenia, historia operacji finansowych, dokumenty związane z korzystaniem z usług bankowości, inwestycje, katy kredytowe, faktury, dokumenty ubezpieczeniowe odnoszące się do statusu materialnego**
(2) **Behawioralne** (świadczące o zachowaniu)	**Np. zwykła historia przeglądania stron internetowych, informacje o lokalizacji (np. z aplikacji do nawigacji), informacje o ruchu sieciowym (bilingi, numer ip), informacje o osobistych nawykach i zwyczajach**
(1) **Proste**	**Np. Imię nazwisko, doświadczenie zawodowe, kwalifikacje, wykształcenie, dane kontaktowe (adres mail, nr telefonu)**

10. Jeżeli naruszenie dotyczyło danych z kategorii:
    - „**Proste**" nadajemy naruszeniu **1 pkt**
    - „**Behawioralne**" nadajemy naruszeniu **2 pkt**

- „**Finansowe**" nadajemy naruszeniu **3 pkt**
- „**Wrażliwe**" nadajemy naruszeniu **4 pkt**

(punkty za kategorie danych nie sumują się, należy przyjąć najwyższą możliwą)

11. Należy uwzględnić kontekst, który może albo podwyższyć wynik (np. z 1 na 4), albo obniżyć wynik (np. z 4 na 1). W każdej sytuacji, w której modyfikujemy wynik bazowy musimy wyraźnie uzasadnić motywy zmiany punktacji.

12. Elementy naruszenia, które zwiększają wynik podstawowy:

- **ilość danych** na temat konkretnej osoby (czy chodzi o pojedynczy dokument, czy zestaw dokumentów, czy chodzi np. o informacje z ostatniego tygodnia, czy ostatniego roku)
- **specyficzny profil działalności** podmiotu, którego naruszenie dotyczyło (czy firma bierze udział w programie zatrudniania osób bezrobotnych, niepełnosprawnych, czy działalność dotyczy np. usług medycznych, czy może świadczyć o światopoglądzie, orientacji itd.)
- **specyficzna rola, sytuacja osoby (lub osób),** których naruszenie dotyczyło (np. wyciek prywatnych numerów telefonów osób powszechnie znanych, np. popularnej drużyny piłkarskiej)

13. Elementy naruszenia, które zmniejszają wynik podstawowy:

- **nieaktualność**, nieprawidłowość danych, np. lista adresowa zawierająca adresy, na które nie mogły być doręczone przesyłki
- **publiczna dostępność** danych, jeżeli przed naruszeniem dany były publicznie dostępne lub z łatwością mogą być zebrane z publicznie dostępnych źródeł
- **natura informacji,** gdy z kontekstu wynika, że w oczywisty sposób informacje nie zaszkodzą osobie lub osobom, której dane dotyczą

Przykład sytuacji, w której kontekst nie podwyższa wyniku:
- kartka z imionami i nazwiskami uczestników standardowego szkolenia firmowego zostaje „wywiana" przez okno. Na kartce były „dane proste", a z samej sytuacji nie wynikają żadne okoliczności dodatkowe.

Przykład sytuacji, w której kontekst podwyższa wynik:
- kartka z imionami i nazwiskami zostaje wywiana przez okno z organizacji zajmującej się pomocą osobom uzależnionym od alkoholu, zestawiając imiona i nazwiska zawarte na kartce ze źródłem, z którego pochodzi, można wywnioskować, że zakres ujawnionej informacji obejmuje osoby uzależnione od alkoholu, dane o nałogach, a więc dane wrażliwe – wynik punktowy ulega zwiększeniu poprzez kontekst z 1 do 4.

Przykład sytuacji, w której kontekst obniża wynik:
Wywiane przez okno lub zgubione zaświadczenie lekarskie o stanie zdrowia Jana Kowalskiego, z którego jednak wynika tylko tyle, że Jan Kowalski jest całkowicie zdrowy. Formalnie jest to informacja dotycząca stanu zdrowia, a więc punktacja bazowa wynosi 4, jednak z kontekstu wynika, że w żaden sposób nie wpłynie to negatywnie na sytuację wspomnianej osoby – inaczej byłoby w przypadku, gdyby z określonego zaświadczenia wynikała określona choroba lub choćby dolegliwości.

14. Po ustaleniu **kategorii informacji (KI)** oraz uwzględnieniu **kontekstu,** należy uwzględnić elementy, które wpływają na **łatwość identyfikacji (ŁI)** (ten czynnik należy uwzględnić przy wyliczaniu **Dotkliwości** wyłącznie w przypadku naruszenia poufności, jeżeli doszło wyłącznie do naruszenia dostępności, należy zastosować punktację wskazaną w pkt 17):

a) **Imię i nazwisko** – przyporządkowujemy wynik punktowy:
0.25 pkt – jeżeli imię i nazwisko są zawarte, ale w skali kraju jest to bardzo popularne nazwisko (np. Jan Kowalski)

0.5 pkt – jeżeli imię i nazwisko są zawarte, i jest to raczej rzadko spotykane w skali kraju nazwisko

0.75 pkt – jeżeli w niewielkim mieście jedynie kilka osób nosi to samo imię i nazwisko, lub wyłącznie jedna osoba (a incydent można powiązać z miejscem zamieszkania)

1 pkt – jeżeli występuje razem z datą urodzenia oraz adresem poczty elektronicznej

b) **Numer dowodu osobistego, paszportu, PESEL**

0.25 pkt – jeżeli w ramach naruszenia ujawniono wyłącznie konkretny numer, bez powiązania go z konkretnym imieniem, nazwiskiem lub innymi informacjami na podstawie których możliwe jest ustalenie tożsamości

0.75 pkt – jeżeli w ramach numeru zawarta jest data urodzenia (jak np. w numerze PESEL) i jest to powiązane z innymi informacjami np. adres zamieszkania lub adres poczty elektronicznej

1 pkt – w przypadku np. skanu dowodu osobistego wraz ze zdjęciem

c) **Numer telefonu, adres zamieszkania**

Jeżeli identyfikacja tożsamości bazuje wyłącznie na jednym z tych czynników:

0.25 pkt – jeżeli naruszenie nie ma charakteru lokalnego, a numeru lub adresu nie ma w publicznie dostępnym rejestrze (np. w książce telefonicznej)

0.5 pkt – jeżeli naruszenie ma charakter lokalny, a numeru lub adresu nie ma w publicznie dostępnym rejestrze (np. w książce telefonicznej), choć z uwagi na lokalny charakter jest możliwe ustalenie tożsamości

1 pkt – jeżeli numer lub adres znajduje się w publicznie dostępnym rejestrze

d) **Adres poczty elektronicznej (mail)**

0.25 pkt – jeżeli mail nie zawiera w sobie dodatkowych danych identyfikacyjnych (np. imienia) i nie jest używany jako główny adres poczty elektronicznej

0.75 pkt – jeżeli mail nie zawiera w sobie dodatkowych danych identyfikacyjnych (np. imienia), ale jest używany jako główny (można go odnaleźć poprzez wyszukiwarkę)

1 pkt – jeżeli zawiera dodatkowe dane identyfikujące i jest używany jako główny (można go odnaleźć poprzez wyszukiwarkę)

e) **Wizerunek (np. zdjęcie)**

0.25 pkt – wizerunek jest niewyraźny (np. pochodzi z kamery przemysłowej ze znacznego dystansu)

0.5 pkt – wizerunek jest niewyraźny, ale zwiera dodatkowe informacje np. o specyficznej lokalizacji lub otoczeniu, które mogą ułatwić identyfikację

0.75 pkt – wizerunek jest dobrej jakości, ale brakuje dodatkowych informacji, które mogą ułatwić identyfikację

1 pkt – wizerunek jest wyraźny i zawiera dodatkowe informacje ułatwiające identyfikację (np. lokalizację, specyficzne otoczenie)

f) **Numer identyfikacyjny, Nick(pseudonim) lub inicjały**

0.25 pkt – jeżeli w żaden sposób z tych informacji nie można wywnioskować powiązania z tożsamością konkretnej osoby

0.5 pkt – jeżeli informacje zawierają w sobie dodatkowe dane np. imię lub są powiązane z mailem

1 pkt – jeżeli z informacji wynika imię i nazwisko

15. Po ustaleniu **Kategorii Informacji (KI)**, uwzględnieniu **Kontekstu** oraz czynników mających wpływ na **Łatwość Identyfikacji (ŁI)** należy uwzględnić **Charakter Naruszenia(CN)**
16. Przyporządkowujemy punkty za **Charakter Naruszenia**:

a) **Naruszenia poufności**

0.25 pkt – jeżeli dane zostały ujawnione ograniczonej liczbie znanych odbiorców

0.5 pkt – jeżeli dane zostały ujawnione nieograniczonej liczbie nieznanych obiorców (np. opublikowane w Internecie)

b) **Naruszenia integralności**

0.25 pkt – jeżeli doszło do wprowadzenia nieprawidłowej informacji, została ona nieprawidłowo wykorzystana, ale istnieje możliwość naprawienia błędu poprzez przywrócenie poprzedniego stanu
0.5 pkt – jeżeli doszło do wprowadzenia nieprawidłowej informacji, została ona nieprawidłowo wykorzystana i nie ma możliwości powrotu do stanu prawidłowego

c) **Naruszenia dostępności**
0.25 pkt – czasowy brak dostępności (informacje można odtworzyć poprzez naprawę, zgranie z kopii zapasowej lub uzyskanie od osoby informacji po raz kolejny)
0.5 pkt – trwała utrata dostępności (nie można żadnym sposobem przywrócić utraconych informacji)

d) **Działanie umyślne**
0.5 pkt – jeżeli naruszenie było efektem celowego działania, do ogólnego wyniku charakteru naruszenia należy dodać 0.5 pkt

17. Jeżeli zdarzenie polega wyłącznie na naruszeniu dostępności lub integralności, zamiast **Łatwości Identyfikacji (ŁI)** przyporządkowujemy punkty za **Trudność Przywrócenia (TP):**
0,5 pkt – jeżeli można przywrócić informację lub prawidłową jej treść w niedługim czasie, bez konieczności współpracy z osobami, których danych naruszenie dotyczyło
1 pkt – jeżeli można przywrócić informację lub prawidłową jej treść w niedługim czasie, ale będzie do wymagało współpracy z osobami, których danych dotyczyło naruszenie
2 pkt – jeżeli bezpowrotnie utracono możliwość przywrócenia informacji lub prawidłowej jej treści
18. Wynik w postaci określenia stopnia dotkliwości otrzymujemy w następujący sposób:
D=KI*ŁI+CN, czyli **D**otkliwość = **K**ategoria **I**nformacji pomnożony przez **Ł**atwość **I**dentyfikacji, dodać **C**harakter **N**aruszenia (*ten wzór stosujemy wyłącznie w sytuacji, w której naruszenie ma charakter naruszenia poufności*)

Np. Jeżeli naruszenie polegało na omyłkowym wysłaniu maila z plikiem z imionami, nazwiskami oraz informacją o wysokości wynagrodzenia własnych pracowników do klientów:
Kategoria Informacji(KI)– 3 pkt *(brak modyfikacji punktacji przez kontekst)*
Łatwość Identyfikacji(ŁI) – 0.75 pkt *(imiona i nazwiska w powiązaniu z miejscem pracy)*
Charakter Naruszenia(CN) – 0.25 pkt *(naruszenie poufności do znanego, zamkniętego kręgu obiorców)*
D=3 * 0,75 +0,25
Dotkliwość (D) = 2.5
Wniosek – **Naruszenie należy zgłosić do organu nadzorczego, ale nie trzeba o nim informować osób, których naruszenie dotyczyło.**

Jeżeli naruszenie polegało wyłącznie na utracie dostępności lub integralności, ale gdy nie doszło do utraty poufności, stosujemy następujący wzór:
D=KI*TP (gdzie TP oznacza Trudność Przywrócenia, o której mowa w pkt 17)

Punktacja	Określenie stopnia dotkliwości	Opis
Poniżej 2 punktów	**NISKA**	Osoby nie odczują naruszenia lub mogą napotkać kilka niedogodności, które pokonają bez problemu (czas poświęcony na ponowne wprowadzanie informacji, chwilowe rozdrażnienie, poirytowanie itp.).
Pomiędzy 2 a 3 punkty	**ŚREDNIA**	Osoby mogą napotkać zauważalne niedogodności, które będą w stanie przezwyciężyć pomimo kilku

		trudności (dodatkowe koszty, odmowa dostępu do usług biznesowych, strach, brak zrozumienia, stres, niewielkie dolegliwości fizyczne itd.)
Pomiędzy 3 a 4 punkty	**WYSOKA**	Osoby mogą napotkać znaczące konsekwencje, które powinny być w stanie przezwyciężyć, choć z poważnymi trudnościami (sprzeniewierzenie funduszy, utrata wiarygodności kredytowej, szkody materialne, utrata zatrudnienia, wezwanie do sądu, pogorszenie stanu zdrowia itp.).
Powyżej 4	**BARDZO WYSOKA**	Osoby mogą napotkać znaczne, a nawet nieodwracalne konsekwencje, których mogą nie przezwyciężyć (trudności finansowe, takie jak znaczny dług lub brak możliwości zatrudnienia, długoterminowe dolegliwości psychologiczne lub fizyczne, śmierć itp.).

19. Wszelkie zdarzenia podlegające badaniu, z powodu uzasadnionego podejrzenia naruszenia ochrony danych osobowych, niezależnie od ostatecznego uznania ich za stwierdzone naruszenia ochrony danych osobowych oraz ich zgłoszenia (lub niezgłoszenia) do organu nadzorczego, należy odnotować w ***Rejestrze naruszeń ochrony danych osobowych***.

Typ naruszenia	Nazwa	Punkty
KI	Proste	1
	Behawioralne	2
	Finansowe	3
	Wrażliwe	4

Elementy naruszenia	Nieaktualność	zmniejsza
Kontekst KI	Publiczna dostępność	zmniejsza
	Natura informacji	zmniejsza
	Ilość informacji	zwiększa
	Specyficzny profil działalności	zwiększa
	Rola, sytuacja osoby	zwiększa

Łatwość identyfikacji	Imię i nazwisko częste	0,25

W przypadku naruszenia poufności ('D=KI*LI+CN)

Wynik	KI	LI	CN
1,25	1	0,75	0,5

Wniosek: nie trzeba zgłaszać

W przypadku wysłania maila z imionami, nazwiskami, wynagrodzeniu własnych pracowników do klientów

Wynik	KI	LI	CN
2,5	3	0,75	0,25

Wniosek: należy zgłosić do organu nadzorczego, nie informujemy osób, których naruszenie dotyczyło

Utrata dostępności, integralności bez utraty poufności (D=KI*TP)

Wynik	KI	TP
2,25	3	0,75

Wniosek: należy zgłosić do organu nadzorczego, nie informujemy osób, których naruszenie dotyczyło

LI	Imię i nazwisko rzadko spotykane	0,5
	Imię i nazwisko bardzo rzadko spotykane	0,75
	Numer dowodu, bez innych danych	0,25
	Numer PESEL	0,75
	Dowód wraz ze zdjęciem (skan)	1
	Numer tel., adres (gdy brak w rejestrze)	0,25
	Numer tel., adres (gdy brak w rejestrze) ale łatwość odnalezienia	0,75
	Adres e-mail (bez innych danych np. imię)	0,25
	Adres e-mail (imię, nazwisko)	0,75
	Adres e-mail (imię, nazwisko, występuje łatwość wyszukania)	1
	Wizerunek niewyraźny	0,25
	Wizerunek niewyraźny lecz zawiera informacje o lokalizacji	0,25
	Wizerunek wyraźny	0,5
	Wizerunek wyraźny i informacje lokalizacyjne	1
	Numer identyfikacyjny, nick, inicjały, gdy nie można powiązać	0,25
	Numer identyfikacyjny, nick, inicjały wraz z imieniem	0,5
	Numer identyfikacyjny, nick, inicjały wraz z imieniem i nazwiskiem	1

W przypadku wysłania maila z imionami, nazwiskami, nr PESEL wynagrodzenia własnych pracowników do klientów

Wynik	KI	LI	CN
3,25	3	1	0,25

Wniosek: należy zgłosić i poinformować osoby których naruszenie dotyczyło

Charakter naruszenia	**Naruszenie poufności**	
CN	Ujawnienie ograniczonej liczbie osób	0,25
	Ujawnienie nieograniczonej liczbie osób	0,5
	Naruszenie integralności	

	Wprowadzenie nieprawidłowej informacji, istnieje możliwość naprawy	0,25
	Wprowadzenie nieprawidłowej informacji, nie istnieje możliwość naprawy	0,5
	Naruszenie dostępności	
	Czasowy brak dostępności (odtworzenie przez naprawę, z kopii zapasowej)	0,25
	Trwała utrata dostępności	0,5
	Działania umyślne (dodajemy)	
	Naruszenie było celowe	0,5

Trudność przywrócenia	Można w niedługim czasie	0,5
TP	Można w niedługim czasie, lecz wymaga współpracy z osobami których naruszenie dotyczyło	1
	Utrata bezpowrotna	2

Załącznik nr 1

PROTOKÓŁ

Nr: .....

naruszenia ochrony danych osobowych

Osoba sporządzająca: .....

Data i godzina poinformowania osoby sporządzającej: .....

Data i godzina rozpoczęcia badania .....

Data i godzina zakończenia badania .....

Data i godzina badanego zdarzenia .....

Data i godzina zatwierdzenia CZĘŚCI I.....

Data i godzina zatwierdzenia CZĘŚCI II.....

CZĘŚĆ I – opis okoliczności faktycznych zdarzenia:

1. **W jaki sposób uzyskano informacje o zdarzeniu oraz ogólny opis okoliczności:**

.....

.....

(informacja od pracownika, klienta, komunikat w systemie informatycznym, wyłamany zamek w szafie itd.)

.....

(jakie osoby zostały przesłuchane przez sporządzającego protokół w celu ustalenia okoliczności zdarzenia)

.....

.....

(ogólny opis okoliczności zdarzenia, wraz z odesłaniem do notatek z rozmów z przesłuchanymi osobami – notatki powinny być podpisane przez te osoby i dołączone do niniejszego protokołu)

2. **Zdarzenie dotyczyło:**

.....

.....

(wskazanie, jakich dokumentów, kartotek, aplikacji, programów lub systemów nośników dotyczyło zdarzenie)

.....

.....

(określenie kategorii osób, których danych dotyczyło zdarzenie np. pracownicy, klienci, kandydaci na pracowników, osoby zapisane na newsletter, osoby zgłaszające reklamacje itd.)

.....

(wskazanie, danych ilu osób dotyczyło zdarzenie)

.....

(przybliżone określenie ilości informacji, których dotyczyło zdarzenie – np. ewidencja zamówień konkretnego klienta z ostatnich 30 dni, 12 miesięcy, pojedyncze zaświadczenie o stanie zdrowia konkretnego pracownika)

.....

.....

(określenie kategorii informacji, jakich dotyczyło zdarzenie – należy wymienić wszystkie kategorie informacji, których zdarzenie mogło dotyczyć np. „imiona, nazwiska, adresy zamieszkania, nr telefonów, adresy poczty elektronicznej, wysokość wynagrodzenia itd.")

3. **Zdarzenie polegało na:**

.....

.....

(-naruszeniu <u>poufności</u> – osoba nieuprawniona uzyskała dostęp do informacji dla niej nieprzeznaczonej
-naruszeniu <u>dostępności</u> – dokument lub informacja uległy utraceniu
-naruszeniu <u>integralności</u> – dane zostały zastąpione, podmienione, błędnie zaktualizowane
-czy działanie było umyślne, czy nieumyślne)

4. **Możliwe konsekwencje zdarzenia dla osób, których danych osobowych zdarzenie dotyczyło:**

   .....
   .....
   .....

   (np. trudności z wypłatą wynagrodzenia na czas, konieczność ponownego wprowadzania danych, wypełniania dokumentów, kradzież tożsamości itd.)

5. **Środki zastosowane w celu zminimalizowania ewentualnych, negatywnych skutków zdarzenia:**

   .....
   .....

   (np. przeglądanie nagrań z monitoringu w celu wykrycia sprawcy, powiadomienie policji, powiadomienie osób, których danych zdarzenie dotyczyło, zmiana haseł, wymiana kluczy, próba odtworzenia danych z kopii zapasowych)

6. **Dodatkowe środki rozważane w celu zminimalizowania ewentualnych, negatywnych skutków zdarzenia:**

   .....
   .....

   (rozważane, ale jeszcze nie zastosowane)

7. **Ocena zdarzenia:**

DOSZŁO DO NARUSZENIA OCHRONY DANYCH OSOBOWYCH

lub

NIE DOSZŁO DO NARUSZENIA OCHRONY DANYCH OSOBOWYCH

CZĘŚĆ II – dokonanie formalnej klasyfikacji incydentu:

(należy uzupełnić zgodnie z zasadami wskazanymi w pkt 9-18)

1. **Punkty przypisane za <u>kategorie informacji</u> (KI), których naruszenie dotyczyło:**

   .....
   .....

   (jak w tabeli w pkt 9 załącznika nr 14)

   Jeżeli kontekst zdarzenia ma wpływ na wyjściową punktację kategorii informacji, uzasadnienie tego wpływu na zwiększenie lub obniżenie wyjściowej punktacji:

   .....
   .....

   (jak w pkt 11-13)

2. **Punkty przypisane za <u>charakter naruszenia</u> (CN):**

   .....
   .....

(jak w pkt 16)

3. **Punkty przypisane za łatwość identyfikacji (ŁI) – tylko, jeżeli doszło do naruszenia poufności:**
   .....
   .....
   (jak w pkt 14 załącznika nr 14, jeżeli naruszenie nie ma charakteru naruszenia poufności, należy pominąć obliczanie łatwości identyfikacji i przejść do punktu kolejnego)

4. **Punkty przyznane za trudność przywrócenia danych (TP) – tylko jeżeli doszło do naruszenia dostępności lub integralności (ale nie poufności)**
   .....
   .....
   (zgodnie z pkt 16)

5. **Obliczenie wyniku punktowego dla naruszenia:**
   a) **W przypadku naruszenia, w ramach którego doszło do naruszenia poufności:**
      D=KI*ŁI+CN
      ...=...*...+...
   b) **W przypadku naruszenia polegającego wyłącznie na utracie dostępności lub integralności, ale gdy nie doszło do utraty poufności:**
      D=KI*TP
      ...=...+....
6. **Słowne określenie stwierdzonej powagi naruszenia:**
   .....
   (zgodnie z tabelą z pkt 18)
7. **Rekomendacja dotycząca stwierdzenia obowiązku poinformowania organu nadzorczego lub osób, których naruszenie dotyczyło**
   .....

Procedura zgłaszania incydentów informatycznych opisana jest w załączniku nr 3. Należy bezwzględnie stosować się do zaleceń organu monitorującego ten typ incydentów.

REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

L.p.	Ogólny opis zdarzenia	Nr protokołu naruszenia	Data zajścia zdarzenia/ /stwierdzenia naruszenia	Osoba sporządzająca protokół	Wynik punktowy klasyfikacji naruszenia	Klasyfikacja naruszenia
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						

Osoba prowadząca: : .....

(miejscowość, data)

UPOWAŻNIENIE DLA ADMINISTRATORA SYSTEMU INFORMATYCZNEGO (ASI)

w Urzędzie Gminy w Jedwabnie

Ja, niżej podpisany ..... jako osoba wykonująca funkcję Administratora Danych Osobowych niniejszym upoważniam do sprawowania funkcji ASI Pana/Panią..... posługującego/cą się numerem PESEL: .....

Do obowiązków ASI w zakresie ochrony danych osobowych, będzie należało wdrożenie i nadzór nad prawidłową realizacją w imieniu ADO Polityki Bezpieczeństwa a w szczególności:

1. Realizację obowiązków w zgodzie z obwieszczeniem Prezesa Rady Ministrów z dnia 14 stycznia 2016 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych

2. Przeprowadzenie i koordynowanie wykonania inwentaryzacji zasobów informatycznych, nadzór nad zasobami.

3. Pomoc przy wykonywaniu szacowania ryzyka poprzez identyfikację podatności elementów mających wpływ na działanie systemu informatycznego oraz zalecanie i sugerowanie stosowania odpowiednich zabezpieczeń, które te podatności mogą ograniczyć lub wyeliminować – przy szczególnym uwzględnieniu bieżącego stanu wiedzy i technologii.

4. Zabezpieczanie dowodów świadczących o okolicznościach potencjalnego naruszenia ochrony danych osobowych oraz możliwe i niezbędne działania służące do zminimalizowania stopnia dotkliwości naruszenia ochrony danych osobowych, jeżeli naruszenie ma charakter informatyczny.

5. Nadawanie i odbieranie dostępów do konkretnych zasobów informatycznych.

.....

Data, podpis i pieczęć Administratora Danych Osobowych

Ja, niżej podpisany/-a, zobowiązuję się do pełnienia obowiązków ASI w oparciu o przepisy wewnętrzne obowiązujące w Urzędzie Gminy w Jedwabnie.,

.....

Data i podpis osoby przyjmującej funkcję ASI

Załącznik nr 18. Upoważnienie do przetwarzania danych

Przedstawiony dokument stanowi wzór który może być modyfikowany w zależności od zmian prawnych lub organizacyjnych. Niezbędne w upoważnieniu jest wystąpienie następujących elementów: danych osoby, zbiorów danych w rozumieniu RODO, oświadczenia osoby o zapoznaniu się oraz klauzuli informacyjnej.

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym jako Administrator Danych – **Wójt Gminy Jedwabno** z siedzibą w Jedwabnie przy ulicy Warmińskiej 2, upoważniam:

Panią .....

do dostępu do danych zawartych w zbiorach danych: .....

Osoba upoważniona obowiązana jest przetwarzać dane osobowe zawarte zbiorze danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków.

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami określonymi w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z 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) wydanymi na jej podstawie aktami wykonawczymi
i obowiązującymi w Urzędzie Gminy w Jedwabnie, wewnętrznymi regulacjami w sprawie ochrony danych osobowych oraz odpowiedzialności cywilnej.

Naruszenie ww. obowiązków może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów określonych w Ustawie o ochronie danych osobowych oraz stanowi ciężkie naruszenie obowiązków pracowniczych, które może być podstawą rozwiązania umowy o pracę w trybie art. 52 Kodeksu Pracy oraz możliwości dochodzenia roszczeń na drodze cywilnej. Upoważnienie jest ważne do odwołania lub zakończenia zatrudnienia.

.....
Data i podpis upoważniającego

.....
Data i podpis osoby upoważnionej

Oświadczenie

Oświadczam, że zapoznałam/em się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w Urzędzie Gminy w Jedwabnie. Przyjmuję do wiadomości zawarte w nich obowiązki w zakresie ochrony danych osobowych i zobowiązuję się do ich stosowania.

Zobowiązuję się także do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam, lub będę miał/-a dostęp w związku z wykonywaniem jakichkolwiek czynności. Zobowiązuję się przestrzegać wszelkich obowiązujących procedur dotyczących ochrony danych osobowych, ze szczególnym uwzględnieniem obowiązku powiadamiania przełożonego o możliwych naruszeniach ochrony danych osobowych.

Świadoma/y jestem obowiązku ochrony danych osobowych na zajmowanym stanowisku i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu upoważnienia, a także po ustaniu zatrudnienia.

.....

Data i podpis osoby upoważnionej

1 x oryginał dokumentacja kadrowa
1 x oryginał osoba upoważniona

Klauzula informacyjna o przetwarzaniu danych osobowych.

Na podstawie art. 13 ust. 1 i 2 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, dalej RODO), informuję o zasadach przetwarzania danych osobowych oraz o przysługujących prawach z tym związanych.

1. Administratorem danych osobowych przetwarzanych w Urzędzie Gminy w Jedwabnie jest Wójt Gminy Jedwabno.
2. Kontakt: Urząd Gminy w Jedwabnie, ul. Warmińska 2, 12-122 Jedwabno, adres e-mail: ug@jedwabno.pl. Do kontaktów w sprawie ochrony danych osobowych został wyznaczony Inspektor Ochrony Danych Cezary Szczepańczyk, z którym można się kontaktować wysyłając e-mail na adres: iod@jedwabno.pl lub w siedzibie administratora.
3. Administrator danych osobowych przetwarza dane osobowe na podstawie obowiązujących przepisów prawa, zawartych umów oraz na podstawie udzielonej zgody.
4. Celem zbierania danych jest ich przetwarzanie w celu realizacji zadań publicznych na warunkach wskazanych w art. 6 ust. 1 lit. a, b, c, d, e. W przypadkach szczególnych mogą być przetwarzane na podstawie art.9 ust.2 lit. a, c RODO. Podanie przez Panią/Pana danych osobowych jest obowiązkowe w sytuacji, gdy przesłankę przetwarzania danych osobowych stanowi przepis prawa lub zawarta między stronami umowa.
5. W związku z przetwarzaniem danych w celach, o których mowa w pkt 4 odbiorcami danych osobowych mogą być:
   a) organy władzy publicznej oraz podmioty wykonujące zadania publiczne lub działające na zlecenie organów władzy publicznej, w zakresie i w celach, które wynikają z przepisów powszechnie obowiązującego prawa,
   b) inne podmioty, które przetwarzają dane osobowe na podstawie umów podpisanych z administratorem.
6. Dane osobowe będą przechowywane przez okres niezbędny do realizacji celów określonych w pkt 4, a po tym czasie przez okres oraz w zakresie wymaganym przez przepisy powszechnie obowiązującego prawa.
7. W związku z przetwarzaniem Pani/Pana danych osobowych przysługują Pani/Panu następujące uprawnienia:
   a) prawo dostępu do danych osobowych, w tym prawo do uzyskania kopii tych danych;
   b) prawo do żądania sprostowania (poprawiania) danych osobowych;
   c) prawo do żądania usunięcia danych osobowych, jeżeli:
   - dane nie są już niezbędne do celów, dla których były zebrane lub w inny sposób przetwarzane,
   - osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania danych osobowych,
   - osoba, której dane dotyczą wycofała zgodę na przetwarzanie danych osobowych, która jest podstawą przetwarzania danych i nie ma innej podstawy prawnej przetwarzania danych,
   - dane osobowe przetwarzane są niezgodnie z prawem,
   - dane osobowe muszą być usunięte w celu wywiązania się z obowiązku wynikającego z przepisów prawa;
   d) prawo do żądania ograniczenia przetwarzania danych osobowych, jeżeli:
   - osoba, której dane dotyczą kwestionuje prawidłowość danych osobowych,
   - przetwarzanie danych jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych, żądając w zamian ich ograniczenia,
   - Administrator nie potrzebuje już danych dla swoich celów, ale osoba, której dane dotyczą, potrzebuje ich do ustalenia, obrony lub dochodzenia roszczeń,
   - osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania danych, do czasu ustalenia czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstawy sprzeciwu;
   e) prawo do przenoszenia danych – w przypadku kiedy łącznie spełnione są następujące przesłanki:
   - przetwarzanie danych odbywa się na podstawie umowy zawartej z osobą, której dane dotyczą lub na podstawie zgody wyrażonej przez tą osobę,
   - przetwarzanie odbywa się w sposób zautomatyzowany;
   f) prawo sprzeciwu wobec przetwarzania danych, jeżeli łącznie spełnione są następujące przesłanki:
   - istnieją przyczyny związane z Pani/Pana szczególną sytuacją, w przypadku przetwarzania danych na podstawie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej przez administratora,
   - 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.
   Jeżeli przetwarzanie danych odbywa się na podstawie zgody osoby, której dane dotyczą, przysługuje jej prawo do cofnięcia tej zgody w dowolnym momencie. Cofnięcie to nie ma wpływu na zgodność przetwarzania, którego dokonano przed cofnięciem zgody.
8. W przypadku powzięcia informacji o niezgodnym z prawem przetwarzaniu danych osobowych, osoba, której dane dotyczą ma prawo wniesienia skargi do organu nadzorczego: Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

Pani/Pana dane nie będą służyły do zautomatyzowanego podejmowania decyzji w tym profilowania.

Retencja

Podczas określania okresu retencji wskazane jest posiłkowanie się dokumentem: Dz.U.11.14.67. ROZPORZĄDZENIE PREZESA RADY MINISTRÓW z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych.

W przypadku podjęcia decyzji o usunięciu danych konieczne jest postępowanie zgodne z Ustawą o *narodowym zasobie archiwalnym i archiwach* (Dz. U. z 2016 r. poz. 1506 ze zm.).

Do newralgicznych obszarów, w których występują dane osobowe o różnym okresie retencji są: informacja publiczna, dane kadrowe czy dane wykorzystywane przy określaniu świadczeń socjalnych i zapomóg. Dane te powinny być przeglądane w cyklach rocznych a sposób postępowania z nimi powinien być zgodny z obowiązującymi przepisami prawa.

Przykładowe okresy retencji, dla danych które nie występują w JRWA.

L.p.	Procesy	Okres retencji
1	Utrzymywanie bazy kontaktów, książek adresowych,	Do momentu istnienia relacji biznesowych
2	Wnioski Podmiotów Danych	10 lat
3	Komunikacja wewnętrzna (intranet)	Dane pracownika (profil użytkownika) – do momentu ustania stosunku pracy, o ile przepisy wewnętrzne nie stanowią inaczej. Poszczególne wiadomości/wydarzenia – w okresie niezbędnym dla uzasadnionych celów.
4	Wysyłka newsletteru	Konieczność ustalenia na jak długo zawierana jest umowa o świadczenie usług drogą elektroniczną, np. z góry określona 3-letnia subskrypcja. Cele obrony przed roszczeniami z tytułu naruszenia dóbr osobistych z uwagi na treść newsletteru – np. 3 lata po ustaniu subskrypcji. Maksymalnie 10 lat

Zasady monitorowania.

Za monitorowanie i sprawdzenie odpowiedzialna jest wskazana przez ADO osoba (np. Inspektor Ochrony Danych).

1. W ramach przygotowywania harmonogramu sprawdzeń w konkretnym roku kalendarzowym należy uwzględnić przede wszystkim te obszary, co do których na jakimkolwiek etapie stwierdzono poziom WYSOKI poziom ryzyka, w ramach przeprowadzania ogólnego szacowania ryzyka.
2. Przy przeprowadzaniu sprawdzeń przestrzegania przez osoby upoważnione do przetwarzania zasad bezpieczeństwa przetwarzania danych osobowych sprawdzenie może polegać w szczególności na:
   - wizytacji i oględzinach na stanowisku pracy ze szczególnym uwzględnieniem stanu i sposobu korzystania z mebli biurowych służących do przechowywania dokumentów lub elektronicznych nośników informacji,
   - dokonaniu dokumentacji fotograficznej obszaru, na którym przetwarzane są dane osobowe,
   - sprawdzeniu sposobów korzystania z urządzeń elektronicznych służących do przetwarzania danych osobowych.
   - ustaleniu, czy faktyczny sposób wykorzystania urządzeń odnotowanych w ramach inwentaryzacji zasobów informatycznych, ich stan i konfiguracja są zgodne z przygotowaną dokumentacją
   - ustaleniu, czy osoba upoważniona przestrzega obowiązku minimalizacji danych, czyli czy przechowuje i gromadzi wyłącznie taki zakres informacji, który jest niezbędny na jej stanowisku do realizacji celu zgodnego z przyjętą podstawą prawną
   - ustaleniu, czy osoba przetwarzająca przestrzega przyjętych terminów przechowywania danych.
3. Podczas przeprowadzanych sprawdzeń należy zwrócić szczególną uwagę na sygnały płynące od osób upoważnionych co do potencjalnych problemów lub zagrożeń związanych z przetwarzaniem danych osobowych na konkretnym stanowisku.
4. Podczas sprawdzeń związanych z przestrzeganiem procedur i przepisów przez osoby upoważnione należy potwierdzić lub uaktualniać dokumenty, w których odnotowano inwentaryzację zasobów informacyjnych i informatycznych.
5. Nie rzadziej niż raz na rok, należy przeprowadzić ponowną, ogólną ocenę prawidłowości podstaw prawnych przyporządkowanych do konkretnych kategorii danych osobowych, ze szczególnym uwzględnieniem krajowych przepisów, jeżeli wskazano je jako podstawę prawną w związku z art. 6 ust. 1 lit. c.
6. Nie rzadziej niż raz na rok, należy ustalić, czy wszystkie kategorie informacji zbierane do tej pory są dalej konieczne do realizacji określonych celów przetwarzania, i czy możliwe jest zrezygnowanie z pozyskiwania poszczególnych kategorii informacji.
7. **Nie rzadziej niż raz na rok**, należy potwierdzić aktualność, lub stwierdzić konieczność sformułowania nowych scenariuszy potencjalnych zagrożeń przeznaczonych do ogólnego szacowania ryzyka.

8. W przypadku dodania nowych scenariuszy zagrożeń należy uzupełnić przeprowadzone uprzednio szacowanie ryzyka, poprzez dodanie nowych protokołów szacowania ryzyka.
9. Raz na kwartał wykonywane jest sprawdzenie stanu wykonania przyjętych planów postępowania z ryzykiem.
10. Raz na 6 miesięcy dokonywane jest sprawdzenie (test) realnego funkcjonowania procedury zgłaszania informacji o potencjalnych naruszeniach ochrony danych osobowych, w ramach którego ewidencjonowane są dostrzeżone uchybienia w funkcjonowaniu tej procedury.
11. Osoby upoważnione, które w przypadku testu, zachowały się niezgodnie z przyjętymi zobowiązaniami – w szczególności nie poinformowały o możliwym naruszeniu przełożonego – upominane są o nieprawidłowości zachowania oraz zobowiązane są do przejścia dodatkowego szkolenia z przepisów i procedur ochrony danych osobowych w ciągu kolejnych 2 tygodni.
12. Osoba dokonująca sprawdzenia przestrzegania przyjętych procedur ochrony danych osobowych dokumentuje sprawdzenie poprzez sporządzenie sprawozdania.

SPRAWOZDANIE

z przestrzegania przyjętych procedur ochrony danych osobowych

Imię i nazwisko osoby dokonującej sprawdzenia: .....

data rozpoczęcia i zakończenia sprawdzenia.....

1. .....
   .....
   (określenie przedmiotu i zakresu sprawdzenia)
2. .....
   .....
   .....
   .....
   .....
   .....
   (wykaz czynności podjętych przez osobę sprawdzającą w toku sprawdzenia oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach)
3. .....
   .....
   .....
   .....
   .....
   .....
   (opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych)

4. .....
   .....
   .....
   .....
   .....
   .....
   (stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem)

Załączniki:

1. .....
2. .....
3. .....

.....
(podpis osoby sprawdzającej)

HARMONOGRAM SPRAWDZEŃ NA ..... ROK.

Osoba odpowiedzialna za wykonanie: .....

L.p.	Przedmiot	Zakres	Termin	Sposób i zakres dokumentowania
1.	*np. jaki dział, biuro program, stanowisko, system jest sprawdzany*	*np. sposób przechowywania dokumentów papierowych, okresy przechowywania dokumentów, sposób niszczenia, zgodność pozyskiwanych danych z podstawami prawnymi*	*np. od 20 do 21 czerwca 2018 roku*	*np. notatka z ustnych wyjaśnień, zrzut z ekranu, fotokopia dokumentu*
2.				
3.				
4.				
5.				
6.				
7.				

Załącznik nr 21. Wyciąg z procedur ochrony danych.

PODSTAWOWE ZASADY OCHRONY DANYCH OSOBOWYCH

(podsumowanie najważniejszych obowiązków związanych z ochroną danych osobowych dostęp do danych osobowych w ograniczonym zakresie).

1. Wszelkie informacje -zarówno w formie papierowej, jak i elektronicznej - pozwalające na identyfikację konkretnej osoby stanowią dane osobowe podlegające ochronie.
2. Każdy pracownik posiadający dostęp do danych osobowych jest zobowiązany do dołożenia szczególnej staranności do zabezpieczenia danych osobowych przed ich zniszczeniem lub udostepnieniem osobom nieuprawnionym.
3. Każdy pracownik, który w ramach swoich obowiązków służbowych posługuje się dokumentami zawierającymi dane osobowe musi przechowywać je w szafach zamykanych na klucz.
4. Dokumentów lub nośników zawierających dane osobowe nie wolno wynosić poza teren zakładu pracy oraz kopiować bez zgody przełożonego.
5. Każdy pracownik może mieć dostęp do danych osobowych wyłącznie w zakresie określonym w upoważnieniu do przetwarzania danych osobowych.
6. Każdy pracownik posiadający dostęp do danych osobowych w formie elektronicznej musi posiadać swój własny login oraz hasło, składające się z co najmniej 8 znaków.
7. Naruszenie procedur zabezpieczenia danych osobowych może skutkować odpowiedzialnością karną, a od 25 maja 2018 roku także nałożeniem na przedsiębiorstwo wielomilionowych kar pieniężnych, co dla pracownika może skutkować odpowiedzialnością dyscyplinarną i cywilną.
8. **Każdy pracownik jest zobowiązany do zgłaszania naruszeń ochrony danych – niezwłocznie do swojego bezpośredniego przełożonego** lub bezpośrednio na nr tel: ..... lub mail: .....@.....
9. Naruszeniem ochrony danych **może być np. zabranie/zgubienie/zniszczenie/kradzież dokumentu zawierającego dane osobowe** a także wykrycie na komputerze złośliwego oprogramowania (wirusy, trojany), uszkodzenie komputera (lub innego urządzenia służącego do pracy na danych osobowych), podobnie jak zgubienie np. służbowego smartfona, laptopa pendrive.
10. Każde naruszenie ochrony danych musi być odnotowane w dokumentacji wewnętrznej przedsiębiorstwa, a część z nich zgłoszona do Urzędu Ochrony Danych.
11. Obowiązek niezwłocznego powiadamiania o fakcie naruszenia ochrony danych jest związany z nałożonym na przedsiębiorcę obowiązkiem powiadamiania w ciągu 72 godzin o naruszeniu Urzędu Ochrony Danych – niedopełnienie tego obowiązku może skutkować nałożeniem na firmę wysokich kar pieniężnych.
12. W celu zminimalizowania ryzyka zainstalowania złośliwego oprogramowania, pracownik nie może na stanowisku komputerowym instalować oprogramowania bez zgody przełożonego.
13. Przestrzeganie zasad ochrony danych podlega cyklicznym sprawdzeniom, każdy pracownik ma obowiązek umożliwić osobie sprawdzającej wyznaczonej przez zarząd dokonanie niezbędnej weryfikacji.
14. Lekceważenie wyżej przywołanych zasad, zwłaszcza w zakresie zgłaszania potencjalnych naruszeń ochrony danych, współpracy przy sprawdzeniach przestrzegania procedur lub odpowiedniego zabezpieczania danych osobowych na swoim stanowisku pracy będzie postrzegane jako przewinienie dyscyplinarne.

Stosujemy się do następujących zasad:

– **Zasada uprawnionego dostępu** – każdy pracownik przechodzi szkolenie z zasad ochrony informacji, spełnia kryteria dopuszczenia do informacji i podpisuje stosowne oświadczenie o zachowaniu poufności.
– **Zasada przywilejów koniecznych** – każdy pracownik posiada prawa dostępu do informacji, ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań.
– **Zasada wiedzy koniecznej** – każdy pracownik posiada niezbędną wiedzę o systemie, do którego ma dostęp tylko w zakresie realizacji powierzonych mu zadań.
– **Zasada świadomości zbiorowej** – wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych i aktywnie uczestniczą w tym procesie poprzez regularne szkolenia.
– **Zasada indywidualnej odpowiedzialności** – każdy pracownik odpowiada za bezpieczeństwo poszczególnych elementów systemu zarządzania bezpieczeństwem informacji.
– **Zasada obecności koniecznej** – prawo przebywania w określonych miejscach mają tylko osoby upoważnione.
– **Zasada stałej gotowości** – niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających.
– **Zasada najsłabszego ogniwa** – poziom bezpieczeństwa wyznacza najsłabiej zabezpieczony element, którym najczęściej jest człowiek (pracownik).
– **Zasada kompletności** – zabezpieczenie jest skuteczne tylko wtedy, gdy stosuje się podejście kompleksowe, uwzględniające wszystkie stopnie i ogniwa ogólnie pojętego procesu przetwarzania informacji.
– **Zasada ewolucji** – każdy system musi ciągle dostosowywać mechanizmy wewnętrzne do zmieniających się warunków zewnętrznych.
– **Zasada świadomej konwersacji** – nie zawsze i wszędzie trzeba mówić, co się wie, ale zawsze i wszędzie trzeba wiedzieć co, gdzie i do kogo się mówi.
– **Zasada zamkniętego pomieszczenia** – ostatnia osoba wychodząca z pomieszczenia na zakończenie dnia pracy jest zobowiązana zamknąć drzwi na klucz. Niedopuszczalne jest pozostawienie otwartych pomieszczeń w godzinach pracy, gdy nikogo upoważnionego nie ma w środku.
– **Zasada nadzorowanych dokumentów** – po godzinach pracy w zamkniętych szafach lub biurkach powinny być przechowywane wszystkie dokumenty, które zostały uznane za informacje istotne dla działania Zakładu.

Załącznik 22. Szkolenia.

Inspektor Ochrony Danych przeprowadza szkolenie z każdym pracownikiem po przyjęciu do pracy. Jest to szkolenie uzupełniające do szkolenia stanowiskowego prowadzonego przez ASI po zatrudnieniu. Szkolenia mogą być prowadzone łącznie.

Z przeprowadzonego szkolenia sporządza się protokół.

PROTOKÓŁ

z przeprowadzenia szkolenia z Ochrony Danych Osobowych w

.....

Osoba prowadząca szkolenie: .....

Data przeprowadzenia szkolenia: .....

Program szkolenia (przykładowy):

1. omówienie ogólne RODO,
2. omówienie aktualnej Ustawy o Ochronie Danych Osobowych,
3. zasady zarządzania informacją,
4. procedury postępowania z dokumentacją tradycyjną (papierową) i elektroniczną.

.....

.....

(imię i nazwisko osoby prowadzącej szkolenie)

Lista osób biorąca w szkoleniu

Imię	Nazwisko	Własnoręczny podpis

I. WPROWADZENIE

Celem niniejszej procedury jest określenie sposobu aktualizacji i usuwania danych osobowych oraz wykonywania obowiązku powiadomienia o ich sprostowaniu, usunięciu lub ograniczeniu przetwarzania. Procedura ta jest dostępna dla wszystkich pracowników, a jej znajomość jest obowiązkowa. Niezbędnym jest również takie dokumentowanie działań, aby zapisy mogły być wykorzystane jako dowód procesowy.

II. ZAKRES

Procedura ta obejmuje realizację procesów aktualizacji oraz usuwania danych osobowych.

III. ZAKRES ODPOWIEDZIALNOŚCI

Dla realizacji niniejszej procedury przewidziane zostały trzy kluczowe role, tj.:

a) Pracownik;
b) IOD;
c) Komórka ds. IT.

IV. Zasada prawidłowości danych osobowych

Obowiązek zapewnienia prawidłowości, aktualności oraz zgodnego z prawem usuwania danych osobowych dotyczy pracowników oraz wszystkich osób zaangażowanych w ich przetwarzanie, a Administrator podejmuje wszelkie możliwe działania, aby ten obowiązek był realizowany. Brak dbałości może nie tylko powodować, że takie dane będą bezużyteczne, ale też mogą działać na niekorzyść Administratora i osób których dane są przetwarzane. Może też narazić Spółkę na znaczne kary finansowe i utratę reputacji.

V. Aktualizacja danych osobowych

1. Prawo do sprostowania oraz uzupełnienia danych

Wnioskodawca ma prawo żądania od Administratora niezwłocznego sprostowania dotyczących danych osobowych. Za dane nieprawidłowe przyjmuje się dane niezgodne z rzeczywistym stanem rzeczy, z punktu widzenia wnioskodawcy, w tym się dane prawidłowe, lecz odzwierciedlające jedynie część rzeczywistego stanu rzeczy.

Administrator, mając na względzie poszczególne cele przetwarzania, zapewnia także realizację żądań w zakresie uzupełnienia niekompletnych danych osobowych.

2. Odpowiedzialność za prawidłowość i aktualizację danych osobowych. Ramy czasowe działań.

Pracownik jest odpowiedzialny za prawidłowość i aktualizację danych osobowych. Jego obowiązkiem jest wykazanie szczególnej staranności przy weryfikacji poprawności i kompletności danych osobowych, także na etapie ich gromadzenia. Ocenia on, z punktu widzenia wnioskodawcy, konsekwencje ewentualnej niedokładności pozyskiwanych danych oraz uwzględnia otrzymane wnioski dotyczące sprostowania a także uzupełnienia niekompletnych danych osobowych, gdy okażą się one zasadne.

Niezwłocznie, oznacza, że gdy natychmiastowa aktualizacja danych osobowych jest zasadna i wykonalna, powinna nastąpić w terminie nie przekraczającym **7** dni roboczych od dnia otrzymania wniosku. W innych przypadkach sprostowanie lub uzupełnienie danych powinno nastąpić w maksymalnym terminie **12** dni roboczych po otrzymaniu żądania.

Pracownik jest odpowiedzialny za zapewnienie, że żądania zostaną skutecznie zrealizowane.

3. Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania

Administrator w ciągu **10** dni roboczych informuje o dokonanym sprostowaniu, uzupełnieniu, usunięciu lub ograniczeniu przetwarzania danych osobowych, każdego odbiorcę, któremu ujawniono dane osobowe, jeśli jest to możliwe. Obowiązek ten ciąży na Administratorze niezależnie od obowiązku poinformowania innych administratorów o wniosku w ramach realizacji „prawa do bycia zapomnianym". Obowiązek powiadomienia dotyczy również podwykonawców dostawców. W tym przypadku Administrator może w drodze umowy, nałożyć obowiązek powiadomienia w jego imieniu na przetwarzającego.

W ramach obowiązku, wnioskodawcy przysługuje uprawnienie do żądania od Administratora informacji o wszystkich, którym zostały ujawnione jego dane osobowe które podlegają sprostowaniu, usunięciu lub ograniczeniu przetwarzania. Administrator informuje o tych odbiorcach w przypadku, gdy wnioskodawca tego zażąda.

Jeżeli realizacja obowiązku okaże się niemożliwa lub będzie wymagać niewspółmiernie dużego wysiłku lub kosztów, w odpowiedzi na żądanie Administrator informuje wnioskodawcę o tych okolicznościach.

Administrator, w przypadkach i na zasadach określonych w dokumencie Realizacja Praw, może pobrać rozsądną opłatę lub odmówić podjęcia działań w związku z żądaniem.

4. Prawo do ograniczenia przetwarzania

W sytuacji, gdy wnioskodawca kwestionuje prawidłowość danych osobowych, ma prawo żądania ograniczenia przetwarzania, na okres pozwalający na sprawdzenie prawidłowości danych.

5. Zasady aktualizowania Danych Osobowych

Wnioskodawca może żądać sprostowania jedynie nieprawidłowych danych osobowych, nie może jednak żądać uzupełnienia dotychczasowych danych danymi nieprawidłowymi. Pracownik jest zobowiązany do oceny wiarygodności danych przekazywanych przez wnioskodawcę. Wnioskodawca powinien także wykazać, że Administrator przetwarza dane nieprawidłowe lub niekompletne.

Nie uwzględnia się żądania dotyczącego sprostowania lub uzupełnienia danych osobowych w sytuacji, gdy wnioskodawca nie udowodnił, że przetwarzane dane są niekompletne lub nieprawidłowe. Nie uwzględniane są również żądania, które zmierzają do uzupełnienia danych osobowych o dane nadmierne w stosunku do celów przetwarzania.

VI. Usuwanie danych osobowych

1. Ograniczenie przechowywania Danych Osobowych

Usuwanie danych jest ważnym elementem procesu przetwarzania danych osobowych. Dane te nie mogą być bowiem przechowywane w formie umożliwiającej identyfikację dłużej niż jest to niezbędne, co wymusza regularne usuwanie danych osobowych lub ich zanonimizowanie.

W ramach określania okresu przechowywania danych osobowych stosuje się sugestie zawarte w Załączniku 19.Retencja a także wskazane jest posiłkowanie się okresem przechowywania danych zawartych w JRWA (Jednolity Rzeczowy Wykaz Akt, opracowany dla jednostek administracji).

Pracownik uwzględnia tryby usuwania danych osobowych:

1) z własnej inicjatywy, w oparciu o harmonogram retencji,
2) z własnej inicjatywy, w związku z regularnym przeglądem,
3) z inicjatywy wnioskodawcy.

2. Usuwanie Danych osobowych z inicjatywy Administratora Danych

Pracownik jest odpowiedzialny za właściwe prowadzenie polityki retencji. Dokonuje co najmniej raz do roku przeglądu przetwarzanych danych osobowych pod kątem konieczności ich usunięcia. Określenie konkretnych terminów przeglądu danych osobowych leży po jego stronie. W ramach okresowego przeglądu, kontroluje również upływ okresu retencji oraz weryfikuje, czy dla danego zbioru nie występują sytuacje uzasadniające zmianę okresu retencji jak np. zmiana przepisów prawa.

3. Realizacja wniosków o usunięcie danych osobowych

Pracownik odpowiedzialny jest za realizację wniosków dotyczących usunięcia danych osobowych. Konieczność ta może wiązać się ze skorzystaniem przez wnioskodawcę z takich uprawnień jak: prawo do sprzeciwu, wycofanie zgody, żądanie usunięcia danych. W sytuacji, gdy nie znajduje on podstaw prawnych dla kontynuowania przetwarzania danych, zobowiązany jest on do ich niezwłocznego usunięcia lub ich zanonimizowania. Fakt usunięcia danych powinien zostać udokumentowany.

4. Trwałe usuwanie danych

Pracownik ma obowiązek usuwania danych osobowych w sposób trwały. Do jego obowiązków należy również wybór sposobu usunięcia danych.

Należy zaznaczyć, że w ramach usuwania danych osobowych możliwa jest również ich anonimizacja. Pracownik powinien zapewnić, że po usunięciu lub dokonaniu anonimizacji danych osobowych, nie istnieją informacje pozwalające odzyskać te dane.

5. Usuwanie danych z kopii bezpieczeństwa

Usuwanie danych osobowych dotyczy także nośników informatycznych stanowiących kopie bezpieczeństwa. Pracownik przy wsparciu komórki IT stosuje rozwiązania, które w ramach realizacji obowiązku usuwania określonych danych osobowych z kopii bezpieczeństwa, nie narażą na zniszczenie czy utratę pozostałych danych.

Pracownik nie ma obowiązku zlecania usuwania danych osobowych z kopii bezpieczeństwa, jeżeli pociągałoby to za sobą niewspółmierne koszty lub miałoby powodować znaczne trudności technologiczne. Takie działanie powinno zostać udokumentowane w sposób możliwie dokładny.

I. WPROWADZENIE

Celem niniejszej Procedury jest określenie sposobu realizacji praw Podmiotów Danych zagwarantowanych przepisami z zakresu ochrony danych osobowych. Procedura ta jest dostępna dla wszystkich pracowników a jej znajomość jest obowiązkowa dla wszystkich pracowników zaangażowanych w przetwarzanie danych osobowych.

II. ZAKRES

Procedura ta obejmuje role, obowiązki i zasady postępowania, zgodnie z przepisami z zakresu ochrony danych osobowych, z prawami i wnioskami osób, których dane osobowe są przetwarzane w organizacji.

III. ZAKRES ODPOWIEDZIALNOŚCI

Szczegółowy zakres odpowiedzialności dotyczącej danego procesu określono w Rozdziale V

IV. Wprowadzenie i zakres

Urząd Gminy zapewnia osobom, których dane osobowe są przetwarzane, realizację ich praw przewidzianych w Przepisach z zakresu ochrony danych osobowych, tj.:

1) prawo do uzyskania informacji, w jaki sposób przetwarzane są ich dane osobowe w organizacji;
2) prawo dostępu do ich danych osobowych;
3) prawo do poprawienia ich danych osobowych;
4) prawo do usunięcia ich danych osobowych (prawo do bycia zapomnianym);
5) prawo do wycofania ich zgody na przetwarzanie ich danych osobowych;
6) prawo do sprzeciwu wobec przetwarzania ich danych osobowych;
7) prawo do przenoszenia danych osobowych;
8) prawo do niepodlegania decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu;
9) prawo do otrzymania informacji w przypadku poważnego incydentu dotyczącego danych osobowych;
10) prawo do ograniczenia przetwarzania danych osobowych;
11) efektywną obsługę wniosków tych osób, gdy wykonują swoje prawa.

Niniejsza procedura opisuje role, obowiązki i zasady postępowania, zgodnie z przepisami z zakresu ochrony danych osobowych. Zakresem niniejszej procedury objęte są wszystkie rodzaje przetwarzania danych osobowych, niezależnie od stosowanych metod, tj. dane osobowe przetwarzane za pośrednictwem systemów informatycznych, a także przetwarzane w inny sposób (np. w arkuszach Excel, w formie papierowej/tradycyjnej). Niniejsza procedura powinna być stosowana przez pracowników oraz osoby trzecie zaangażowane w przetwarzanie danych osobowych w imieniu organizacji.

V. Role i obowiązki

1. Podział ról

Dla realizacji niniejszej procedury przewidziane zostały trzy kluczowe role, tj.:

1) Pracownik odpowiedzialny za przetwarzanie danych osobowych;
2) IOD;
3) Komórka ds. IT.

2. IOD

IOD jest zaangażowany we wszystkie procesy związane z obsługą wniosków Podmiotów Danych. Do ich obowiązków należą wszystkie nieprzypisane innemu podmiotowi sprawy z zakresu realizacji praw Podmiotów Danych, w szczególności:

1) zapewnianie wsparcia dla Właściciela Biznesowego w zakresie obsługi wniosków;
2) przekazywanie wniosków do właściwego Właściciela Biznesowego oraz monitorowanie realizacji wniosków;
3) w przypadku poważnego incydentu związanego z naruszeniem ochrony danych, poinformowanie Podmiotów Danych i poinformowanie o tym Organu Nadzorczego, w razie potrzeby, oraz koordynowanie postępowania w sprawie incydentu.

3. Pracownik

Zadania Pracownika obejmują:

1) niezwłoczne rozpatrywanie wniosków Podmiotów Danych (zapoznawanie się, analiza sprawy, decyzja o podjęciu/odmowie podjęcia czynności objętych żądaniem, sporządzanie i wysyłanie odpowiedzi);
2) angażowanie wszystkich zainteresowanych stron w zakresie obsługi/realizacji wniosków Podmiotów Danych, w uzgodnieniu z IOD;
3) raportowanie do IOD lub uzyskiwanie konsultacji w sprawie działań następczych w związku z wnioskami Podmiotów Danych.

4. Komórka ds. IT

Komórka ds. IT jest zobowiązana wspierać Pracownika w ramach realizacji praw Podmiotów Danych wszędzie, gdzie przetwarzanie odbywa się w systemach informatycznych, np.:

1) określać formaty plików zawierających przenoszone dane;
2) generować ww. pliki w tych formatach i przekazywać je do Podmiotów Danych;
3) usuwać dane;
4) konsultować z Właścicielem Biznesowym kwestie techniczne.

Osobą odpowiedzialną po stronie komórki ds. IT jest osoba zarządzająca tą komórką.

VI. Prawa Podmiotu Danych

Niniejszy rozdział określa prawa Podmiotów Danych.

1. Prawo do otrzymania przejrzystej informacji

W sytuacji, kiedy Urząd Gminy komunikuje się z Podmiotami Danych w kwestii przetwarzania ich Danych osobowych, powinno się to odbywać w zwięzłej, przejrzystej i łatwo dostępnej formie, używając jasnego i prostego języka. Za treść i formę przekazu odpowiada każdorazowo Pracownik. Jako zasadę przyjmuje się, że informacje na temat przetwarzania Danych osobowych przekazywane są Podmiotom Danych za pośrednictwem klauzul, z którymi Podmioty Danych powinny się zapoznać.

2. Prawo dostępu do informacji

Podmiot Danych musi mieć zagwarantowane prawo dostępu do swoich danych osobowych, aby mieć świadomość przetwarzania i móc zweryfikować zgodność przetwarzania z prawem. Podmiot Danych ma prawo do otrzymania potwierdzenia czy dane osobowe jego dotyczące są przetwarzane i w jaki sposób. Jeśli ma to miejsce, Podmiot Danych może zawnioskować

o dostęp do następujących informacji, które udostępnia Pracownik w odpowiedzi na wniosek:

1) cel przetwarzania,
2) kategorie Danych osobowych – a w odniesieniu do danych podstawowych takich jak np. dane identyfikacyjne, dane kontaktowe, dane adresowe, dane o firmie, dane dotyczące umowy, dane organizacyjne związane z pracą – o treści tych informacji;
3) Odbiorcy, którym dane osobowe były lub będą ujawnione,
4) przewidywany okres, przez który dane osobowe będą przechowywane,
5) informacje o prawie do żądania od Administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania, prawo do przenoszenia danych osobowych, prawo do niepodlegania decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu;
6) prawo do złożenia skargi do Organu Nadzorczego,
7) jeżeli dane osobowe nie zostały zebrane od Podmiotu Danych – wszelkie dostępne informacje o ich źródle,
8) możliwe istnienie automatycznego podejmowania decyzji w oparciu o wykorzystanie danych osobowych.

Podmiot Danych może zażądać kopii przetwarzanych danych osobowych. Pracownik dostarcza osobie, której dane dotyczą, jedną kopię danych osobowych podlegających przetwarzaniu. W przypadku, gdy Podmiot Danych zwraca się o kopię drogą elektroniczną i nie zażąda formy pisemnej, informacji udziela się drogą mailową. Niezależnie od udzielenia odpowiedzi, Pracownik zwraca się w ciągu 5 dni roboczych do komórki ds. IT o sporządzenie kopii danych. Komórka właściwa ds. IT ma 3 dni robocze na przekazanie kopii danych do Pracownika, który po weryfikacji przesyła ją do Podmiotu Danych. W sytuacji, gdy kopia jest sporządzona w formie pisemnej (tradycyjnej), wówczas jest przekazywana do Pracownika, który wysyła kopię do Podmiotu Danych.

Kopia danych jest przekazywana wraz z odpowiedzią na wniosek bez opłat. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, Administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych.

3. Prawo do sprostowania i uzupełnienia

Podmiot Danych ma prawo do sprostowania jego nieaktualnych lub niedokładnych Danych osobowych, a także do ich uzupełnienia w przypadku, gdy są niekompletne. Merytoryczne przesłanki oraz procedura realizacji żądań sprostowania lub uzupełnienia Danych osobowych zostały opisane w *Załączniku 23. Aktualizacja i usuwania danych osobowych.* Obsługa wniosków i udzielanie odpowiedzi są realizowane zgodnie z niniejszą procedurą.

4. Prawo do wycofania zgody

Podmiot Danych ma prawo do wycofania zgody w każdym momencie. Obsługa wniosków i udzielanie odpowiedzi są realizowane zgodnie z niniejszą procedurą.

5. Prawo do usunięcia

Podmiot Danych ma prawo do usunięcia jego danych osobowych, znane także jako „prawo do bycia zapomnianym". Dla uzasadnienia żądania usunięcia Danych osobowych spełnione muszą zostać następujące warunki:

1) Dane osobowe nie są już niezbędne do realizacji celów, dla których zostały zgromadzone lub przetwarzane;
2) W przypadkach, w których zgoda Podmiotu Danych była warunkiem przetwarzania, a Podmiot Danych wycofał swoją zgodę, i nie ma innego celu i innej podstawy prawnej przetwarzania (np. prawnie uzasadnionego interesu w trzymaniu danych dla określonych celów);
3) Podmiot Danych sprzeciwia się przetwarzaniu i nie ma żadnych nadrzędnych uzasadnionych przesłanek do przetwarzania lub sprzeciw dotyczy przetwarzania na cele marketingu bezpośredniego (w takim wypadku sprzeciw jest realizowany bezwzględnie);
4) Dane osobowe przetwarzane są niezgodnie z prawem;
5) Dane osobowe muszą zostać usunięte w celu wykonania obowiązków prawnych.

Za realizację wniosków Podmiotów Danych dotyczących usunięcia ich Danych osobowych odpowiedzialny jest Pracownik. Jeżeli organizacja publicznie udostępniła dane osobowe (np. zamieściła na publicznie dostępnej stronie internetowej czy w dokumentach, do których dostęp może mieć nieoznaczony krąg osób), w przypadku uzasadnionego żądania przez Podmiot Danych usunięcia danych osobowych, Pracownik musi, biorąc pod uwagę dostępną technologię i koszty realizacji, podjąć z własnej inicjatywy rozsądne działania, aby poinformować wszystkie inne podmioty, które przetwarzają Dane Osobowe dla własnych celów (administratorów), że Podmiot Danych zażądał usunięcia Danych osobowych.

Administrator może odmówić uwzględnienia wniosku o usunięcie danych w sytuacji, gdy dysponuje inną podstawą prawną niż zgoda podmiotu danych i przetwarza dane w innym celu niż objętym zgodą. Przykładowo przetwarzanie może być niezbędne do celów dochodzenia roszczeń lub wywiązania się z prawnego obowiązku spoczywającego na Administratorze.

Jeżeli realizacja działań okaże się pod względem posiadanej technologii niemożliwa lub będzie wymagać niewspółmiernie wysokich kosztów (np. konieczności dokonania najpierw inwestycji w specjalną infrastrukturę), Pracownik w porozumieniu z IOD może odmówić uwzględnienia realizacji tego prawa.

W zakresie procesu usuwania Danych osobowych na skutek uwzględnienia wniosku stosuje się regulacje *Aktualizacji i usuwania danych osobowych.*

6. Prawo do ograniczenia przetwarzania

Podmiot Danych może żądać ograniczenia przetwarzania danych osobowych w następujących sytuacjach:

1) gdy kwestionuje prawidłowość danych osobowych – na okres pozwalający Administratorowi Danych sprawdzić prawidłowość tych danych;
2) przetwarzanie jest niezgodne z prawem, a Podmiot Danych sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
3) Administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne Podmiotowi Danych do ustalenia, dochodzenia lub obrony roszczeń;
4) Podmiot Danych wniósł sprzeciw wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie Administratora Danych są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

Ograniczenie przetwarzania oznacza, że Administrator nie dokonuje, na objętych ograniczeniem danych osobowych, innych operacji niż przechowywanie, chyba że Podmiot Danych na takie inne operacje wyrazi zgodę. W czasie trwania ograniczenia przetwarzania Administrator Danych zachowuje, jednakże prawo do dokonywania na danych osobowych innych operacji niż przechowywanie, jeżeli jest to niezbędne w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej.

Przykładem ograniczenia przetwarzania może być czasowe przeniesienie wybranych danych osobowych do innego systemu przetwarzania, uniemożliwienie użytkownikom dostępu do wybranych danych lub czasowe usunięcie opublikowanych danych ze strony internetowej.

Dane osobowe, których przetwarzanie ograniczono, powinny być wyraźnie odróżnione od pozostałych danych. Powyższe oznacza, że Pracownik w odniesieniu do:

1) dokumentacji w formie tradycyjnej – przenosi te dokumentacji do zamykanej szafki przeznaczonej dla dokumentów, zawierających dane osobowe objęte ograniczeniem przetwarzania;
2) dokumentacji elektronicznej (plików) – powinny zostać przeniesione do dedykowanego folderu;
3) Danych osobowych w systemach – oflagowane jako objęte ograniczeniem.

W przypadku ograniczenia przetwarzania danych osobowych należy uwzględnić realizację obowiązku informowania Odbiorców, którym ujawniono dane osobowe, zgodnie z dokumentem *Aktualizacja i usuwanie danych osobowych.*

W sytuacji, gdy Właściciel Biznesowy, po analizie treści żądania, celów przetwarzanych danych osobowych i podstaw prawnych tego przetwarzania stwierdzi, że wniosek o ograniczenie przetwarzania zasługuje na uwzględnienie, takie ograniczenie powinno nastąpić w czasie nie dłuższym niż 5 dni roboczych od otrzymania wniosku przez Właściciela Biznesowego.

Pracownik wznawia przetwarzanie danych osobowych w pełnym zakresie w najkrótszym możliwym terminie, w przypadku cofnięcia żądania ograniczenia przetwarzania albo ustania przesłanek – jeżeli ma podstawy prawne do dalszego przetwarzania tych danych – w przeciwnym razie powinien zaprzestać ich przetwarzania. Pracownik zawiadamia Podmiot Danych, który uzyskał takie ograniczenie przetwarzania Danych osobowych, zanim ograniczenie przetwarzanie zostanie uchylone. Oznacza to, że:

1) gdy Podmiot Danych kwestionuje prawidłowość danych - po sprawdzeniu ich prawidłowości przez Właściciela Biznesowego (ewentualnym sprostowaniu, uzupełnieniu);
2) gdy przetwarzanie jest niezgodne z prawem, a Podmiot Danych sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania – po cofnięciu tego żądania albo otrzymaniu od Podmiotu Danych żądania usunięcia ww. danych (pisemnie, mailowo);
3) gdy Pracownik nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne Podmiotowi Danych do ustalenia, dochodzenia lub obrony roszczeń – po otrzymaniu informacji (pisemnej, mailowej) od Podmiotu Danych, że nie są jej/jemu już potrzebne dla tych celów;
4) gdy Podmiot Danych wniósł sprzeciw wobec przetwarzania – po dokonaniu przez Właściciela Biznesowego analizy i stwierdzeniu, czy istnieją/nie istnieją prawnie uzasadnione podstawy po stronie Administratora Danych, które są nadrzędne

wobec podstaw sprzeciwu Podmiotu Danych albo cofnięciu przez Podmiot Danych sprzeciwu (pisemnie, mailowo);

Pracownik w ciągu 2 dni roboczych od momentu otrzymania cofnięcia wniosku/ustania przesłanek do ograniczenia przetwarzania informuje IOD drogą mailową o zamiarze wznowienia przetwarzania danych osobowych przekazując jednocześnie projekt zawiadomienia Podmiotu Danych. I IOD powinien w tym czasie wyrazić swoje stanowisko, formułować zalecenia. W oparciu o te zalecenia Pracownik może zmienić swoją decyzję.

Właściciel Biznesowy, uwzględniając stanowisko IOD, w ciągu 2 dni roboczych od zawiadomienia IOD przekazuje do Podmiotu Danych zawiadomienie o zamiarze uchylenia ograniczenia przetwarzania i w konsekwencji planowanym wznowieniu przetwarzania lub zaprzestaniu przetwarzania danych osobowych.

Uchylenie ograniczenia przetwarzania następuje w ciągu 14 dni od dnia przekazania (wysłania) zawiadomienia do Podmiotu Danych.

W sytuacji realizacji prawa do ograniczenia przetwarzania lub wznowienia przetwarzania w systemach, Pracownik jest obowiązany współdziałać z komórką ds. IT, która niezwłocznie po ograniczeniu/wznowieniu przetwarzania w systemach, potwierdza ten fakt Właścicielowi Biznesowemu drogą mailową.

7. Prawo do przenoszenia danych

Prawo Podmiotu Danych do przenoszenia danych składa się z trzech elementów:

1) Podmiot Danych ma prawo otrzymać kopię swoich danych osobowych, które dostarczył Administratorowi Danych „w ustrukturyzowanym i powszechnie używanym formacie do odczytu maszynowego";
2) Podmiot Danych może przekazać dane osobowe, które otrzymał, do dowolnego innego administratora;
3) Podmiot Danych może żądać od Administratora Danych przekazania jego/jej danych osobowych bezpośrednio do tego innego administratora, jeżeli jest to technicznie wykonalne.

Podmiot Danych może korzystać z tego prawa tylko wtedy, gdy przetwarzanie jego/jej danych osobowych obywa się w sposób zautomatyzowany i opiera się na zgodzie lub umowie. Prawo to nie ma zastosowania w przypadku, gdy przetwarzanie opiera się, na przykład, na uzasadnionym interesie Administratora Danych (np. w zakresie dochodzenia roszczeń) lub na realizacji obowiązków prawnych.

Prawo do przenoszenia danych obejmuje jedynie dane aktywnie i świadomie dostarczane przez Podmiot Danych oraz dane zaobserwowane przez Administratora w związku z korzystaniem z usług lub urządzeń przez Podmiot Danych. Szczegółowy zakres danych, który podlega przenoszeniu jest ustalany przez Właściciela Biznesowego w porozumieniu z IOD. Prawo do przenoszenia dotyczy danych osobowych przetwarzanych w sposób zautomatyzowany i nie dotyczy w szczególności zbiorów prowadzonych w formie tradycyjnej.

W przypadku żądań przenoszenia danych, Pracownik zachowuje szczególną ostrożność przy weryfikacji tożsamości wnioskodawcy. W przypadku żądania przeniesienia danych z serwisu internetowego, żądanie jest realizowane wyłącznie poprzez ten serwis internetowy na żądanie zalogowanego w nim użytkownika wysłane za pośrednictwem tego serwisu.

Określenie „ustrukturyzowany i powszechnie używany format do odczytu maszynowego" pozostawia po stronie komórki ds. IT swobodę w sprecyzowaniu stosowanego formatu plików (np. XLS, XML, JSON, CSV itp.) mając na uwadze interoperacyjność, powszechność ich stosowania oraz wysoką szczegółowość metadanych jako dobrą praktykę. W miarę możliwości komórka ds. IT korzysta z otwartych formatów plików.

W przypadku decyzji Właściciela Biznesowego o realizacji prawa do przenoszenia Danych osobowych, poza konsultacją z IOD, zwraca się on do komórki ds. IT z pytaniem o techniczną wykonalność żądania oraz prośbą o niezwłoczne wygenerowanie i przekazanie zgodnie z wnioskiem plików zawierających przenoszone dane. Komórka a ds. IT ma 10 dni roboczych na realizację takiej prośby.

Od momentu, w którym wniosek o przeniesienie od Podmiotu Danych został złożony, Administrator Danych może nadal przetwarzać dane osobowe, jeżeli w dalszym ciągu istnieją ku temu uzasadnione podstawy. Przenoszenie danych nie powoduje automatycznie usunięcia danych osobowych z systemów lub plików oraz nie ma wpływu na pierwotny okres przechowywania danych osobowych.

Realizacja prawa do przeniesienia danych osobowych poprzez przesłanie danych bezpośrednio innemu administratorowi uzależniona jest od aktualnych możliwości technicznych. Nie ma obowiązku realizacji takiego żądania, w sytuacji, gdyby wiązało się to z obowiązkiem wdrożenia nowych rozwiązań technicznych, czy zakupem nowego oprogramowania dla celów wprowadzenia kompatybilnych technicznie systemów przetwarzania.

Realizacja prawa do przeniesienia danych osobowych nie może powodować uszczerbku dla praw i wolności innych osób niż Podmiot Danych, jeżeli określony zestaw danych odnosi się do różnych osób.

8. Prawo do sprzeciwu

Podmiot Danych ma prawo do sprzeciwu wobec przetwarzania jego/jej danych osobowych, z przyczyn związanych z jej szczególną sytuacją, w szczególności na następujących podstawach:

1) przetwarzanie jest oparte na prawnie uzasadnionym interesie. W przypadku sprzeciwu Pracownik musi zaprzestać przetwarzania danych osobowych, chyba że Pracownik jest w stanie wykazać istotne, uzasadnione podstawy dla przetwarzania, które przeważa nad interesami, prawami i wolnościami Podmiotu Danych (takich jak np. konieczność sprawnego i terminowego dochodzenia roszczeń, kontrola jakości wykonywanych usług itp., które to obiektywnie powinny mieć pierwszeństwo nad niedogodnością po stronie Podmiotu Danych w związku z dalszym przetwarzaniem);
2) sprzeciw dotyczy marketingu bezpośredniego (w tym profilowania) opartego na uzasadnionym interesie – w takim przypadku Podmiot Danych ma prawo w każdej chwili zgłosić sprzeciw, a przetwarzanie danych osobowych w tym celu musi zostać natychmiast zaniechane.

W sytuacji, gdy decyzje dotyczące Podmiotów Danych są podejmowane na podstawie zautomatyzowanych systemów informatycznych, może dojść do naruszenia interesów Podmiotu Danych. Takie decyzje mogą znacząco wpłynąć na Podmiot Danych i/lub wywrzeć dla niego/niej skutki prawne. Zasadą jest, że Podmiot Danych ma prawo nie podlegać takiej

decyzji, która opiera się wyłącznie na automatycznym Przetwarzaniu jego/jej Danych osobowych.

Podmiot Danych nie będzie mógł skorzystać z prawa do niepodlegania zautomatyzowanej decyzji w związku z profilowaniem tylko w ściśle określonych okolicznościach: jeżeli jest to dozwolone przez prawo, jest to niezbędne do zawarcia i wykonania umowy z Podmiotem Danych lub Podmiot Danych wyraził zgodę. W dwóch ostatnich przypadkach Podmiot Danych ma prawo do uzyskania interwencji ludzkiej ze strony Administratora Danych, a także do wyrażenia własnego stanowiska i zakwestionowania decyzji.

W sytuacji skutecznego wniesienia sprzeciwu, gdy brak jest innych podstaw przetwarzania danych osobowych, dane te powinny zostać usunięte zgodnie z *dokumentem Aktualizacja i usuwanie danych osobowych.* W szczególności niedopuszczalne jest pozostawienie w danej bazie imienia i nazwiska osoby oraz numer PESEL lub adresu, wyłącznie w celu uniknięcia ponownego wykorzystania danych tej osoby w celach objętych sprzeciwem.

VII. Obsługa wniosków od Podmiotów Danych

Obsługa wniosków pochodzących od Podmiotów Danych przebiega wg kroków opisanych poniżej.

1. Sposób składania wniosku

Jeżeli Podmioty Danych chcą skorzystać z przysługujących im praw, muszą przesłać swoje wnioski na adres e-mail lub drogą pocztową. Dane kontaktowe do IOD zostaną zawarte w ramach informacji przedstawianych Podmiotowi Danych (obowiązek informacyjny).

Pracownik jest odpowiedzialny za zapewnienie, że wyżej wspomniane dane kontaktowe są łatwo dostępne dla Podmiotów Danych. Pracownik może w tym celu wymagać wsparcia ze strony IOD.

Jeżeli Podmiot Danych złoży pisemny wniosek, Pracownik jest zobowiązany taki wniosek przyjąć, a także w ciągu 2 dni roboczych przekazać (przesłać) do IOD.

Wnioski, które trafiają na skrzynkę IOD, są przekierowywane do właściwego Właściciela Biznesowego w ciągu 1 dnia roboczego.

2. Weryfikacja tożsamości

Zanim wnioskowi Podmiotu Danych zostanie nadany bieg, tożsamość Podmiotu Danych musi zostać zweryfikowana. Pracownik dokonuje weryfikacji tożsamości na podstawie każdorazowej indywidualnej oceny sytuacji. Podmiot Danych powinien na żądanie przedstawić dalsze dane dla ich porównania z danymi posiadanymi przez Właściciela Biznesowego, rejestruje on wtedy datę kontroli tożsamości.

Pracownik nie podejmuje działań w sytuacji, gdy brak jest możliwości weryfikacji, czy żądanie jest składane przez nieuprawniony podmiot (Podmiot Danych). Pracownik – o ile jest możliwy kontakt z nadawcą wniosku - udziela niezwłocznej odpowiedzi o odmowie podjęcia działań.

Jeżeli w związku z przetwarzaniem Danych osobowych zostały osiągnięte założone cele i w związku z tym przetwarzane dane zostały pozbawione cech danych osobowych (np. zanonimizowane) lub usunięte, Pracownik nie ma obowiązku uzyskania dodatkowych informacji w celu identyfikacji Podmiotu Danych. Jeżeli Pracownik może wykazać, że nie jest

w stanie zidentyfikować Podmiotu Danych, w miarę możliwości informuje o tym Podmiot Danych. Wniosek należy rozpoznać w przypadku dostarczenia przez wnioskodawcę danych pozwalających go zidentyfikować.

3. Zaangażowanie IOD – raportowanie przez Właściciela Biznesowego

Pracownik konsultuje się z IOD w każdym przypadku wątpliwości lub pytań odnośnie postępowania z wnioskiem.

W ciągu 3 dni roboczych otrzymaniu wniosku Pracownik przesyła na wewnętrzny adres mailowy IOD informację o otrzymanym wniosku Podmiotu Danych. Informacja zawiera:

1) datę wpływu wniosku;
2) kopię wniosku.

Obowiązek ten nie ma zastosowania, gdy Pracownik otrzymał wniosek, który trafił na skrzynkę IOD i został przez przekierowany do Właściciela Biznesowego.

W ciągu 5 dni roboczych Pracownik przesyła na wewnętrzny adres mailowy IOD informację o zamiarze podjęcia czynności na wniosek np. usunięcia/sprostowania/uzupełnienia/ograniczenia przetwarzania oraz zakresie, planowanej dacie i godzinie wykonania ww. czynności – jeżeli taka jego decyzja

W ciągu 5 dni roboczych od otrzymania wniosku Pracownik przesyła na wewnętrzny adres mailowy IOD projekt odpowiedzi dla Podmiotu Danych wraz z uzasadnieniem.

W ciągu 12 dni roboczych od daty, w której Pracownik udzielił odpowiedzi częściowej Pracownik przesyła na wewnętrzny adres IOD projekt odpowiedzi ostatecznej wraz z uzasadnieniem. Jeżeli Podmiot Danych nie precyzuje wniosku zgodnie z w ciągu 10 dni roboczych od otrzymania żądania sprecyzowania, projekt ostatecznej odpowiedzi jest wysyłany w ciągu 5 dni roboczych od otrzymania odpowiedzi Podmiotu Danych.

Od momentu otrzymania informacji o zamiarze podjęcia kroków lub otrzymania projektu odpowiedzi IOD w ciągu 2 dni roboczych powinien zająć stanowisko, wnieść zastrzeżenia etc. i przez ten czas Pracownik wstrzymuje się z podjęciem dalszych kroków. Stanowisko IOD nie jest dla Właściciela Biznesowego wiążące, jednak każdorazowo Pracownik sporządza notatkę, w która jest włączana do materiału danej sprawy. W notatce Pracownik odnotowuje czy IOD zgłosił uwagi, czy zostały uwzględnione lub jakie były przyczyny ich nieuwzględnienia. Jeżeli Pracownik nie ma udokumentowanego stanowiska IOD (np. kopii wiadomości e-mail) wówczas pod notatką musi złożyć podpis IOD.

Pracownik w ciągu 1 dnia roboczego informuje drogą mailową IOD o podjętych krokach i przesyła skany pism wysłanych do Podmiotów Danych drogą tradycyjną. W przypadku pism wysyłanych do Podmiotów Danych mailowo, każda wiadomość jest wysyłana do wiadomości IOD.

4. Analiza wniosku, przygotowanie odpowiedzi

Pracownik odpowiada za obsługę wniosków. Odpowiedzialność obejmuje zapewnienie, że właściwe informacje związane z wnioskiem (w tym dane osobowe w przypadku wniosku o dostęp lub przeniesienie) zostaną wydobyte z zasobów organizacji, a odpowiedzi na wniosek zostaną dostarczone w przyjętych ramach czasowych.

W przypadku wniosku o dostęp lub przeniesienie, Pracownik jest odpowiedzialny za:

1) przegląd wszystkich informacji i danych osobowych, które zostaną przekazane Podmiotowi Danych w celu odpowiedzi na jego/jej wniosek,
2) sprawdzenie w takich informacjach i danych osobowych, czy obejmują one dane o osobie trzeciej,
3) dopilnowanie, aby informacje lub dane osobowe związane z taką osobą trzecią nie znalazły się w odpowiedzi, która zostanie przekazana Podmiotowi Danych albo uzyskanie pisemnej zgody tej osoby trzeciej, aby informacje i dane osobowe dotyczące tej osoby zostały ujawnione w odpowiedzi na wniosek.

W żadnym wypadku Pracownik nie może zmieniać ani niszczyć danych osobowych w celu uniknięcia ich dostarczenia, jeśli zapytanie Podmiotu Danych dotyczy dostępności lub przenoszalności.

W ramach przygotowania odpowiedzi dla Podmiotu Danych, Pracownik musi sprawdzić, czy istnieją okoliczności, które wpłynęłyby na zakres odpowiedzi i ewentualny brak obowiązku spełnienia żądania wniosku Podmiotu Danych.

W przypadku, gdy Pracownik dostrzega brak obowiązku spełnienia żądania wniosku, ma on obowiązek konsultacji z IOD który wyraża swoje stanowisko nie mające jednak charakteru wiążącego.

W przypadku, gdy wniosek wiąże się z przekazaniem mu danych osobowych (np. wniosek o dostęp lub przeniesienie), Pracownik musi wcześniej ustalić wraz z IOD format, w którym dane osobowe będą dostarczone.

Pracownik wysyła odpowiedzi/inne pisma do Podmiotu Danych (drogą mailową, tradycyjną), na wniosek Podmiotu Danych odpowiedź może być udzielona ustnie, zaś kopię odpowiedzi przekazuje do IOD.

5. Udzielenie odpowiedzi Podmiotowi Danych

Pracownik udziela odpowiedzi (informacji o działaniach podjętych w związku z żądaniem, potwierdzenia przetwarzania danych, przekazania danych w ramach prawa dostępu) Podmiotowi Danych bez zbędnej zwłoki, nie później jednak niż w ciągu miesiąca od otrzymania wniosku.

Z uwagi na konieczność sprecyzowania terminu „bez zbędnej zwłoki" w stopniu zapewniającym największe poszanowanie przepisów RODO, IOD oraz Pracownik zobowiązani są do stosowania się do szczegółowych terminów wskazanych poniżej.

Niezależnie od udzielenia odpowiedzi (informacji o działaniach podjętych w związku z żądaniem, potwierdzenia przetwarzania danych, udzielenia informacji/przekazania danych w ramach prawa dostępu do danych osobowych), w przypadku złożenia zasadnych wniosków dotyczących:

1) sprostowania i uzupełnienia danych,
2) usunięcia danych,
3) ograniczenia przetwarzanych,
4) wycofania zgody

Pracownik niezwłocznie prostuje, uzupełnia, usuwa dane osobowe, ogranicza ich przetwarzanie lub realizuje wycofanie zgody. Szczegółowe terminy na sprostowanie, uzupełnienie i usunięcie Danych osobowych wskazane są w dokumencie *Aktualizacja i*

usuwanie danych osobowych. W przypadku zasadności wniosku o ograniczenie przetwarzania danych osobowych, takie ograniczenie powinno nastąpić w czasie nie dłuższym niż 5 dni roboczych od otrzymania wniosku przez Właściciela Biznesowego.

Pracownik musi wysłać odpowiedź na wniosek Podmiotu Danych w ciągu 8 dni roboczych od daty otrzymania przez Właściciela Biznesowego tego wniosku. Możliwe jest udzielenie odpowiedzi częściowej.

Odpowiedź na wniosek Podmiotu Danych może być albo ostateczna (potwierdzenie faktu przetwarzania danych, dostarczenie wszystkich wnioskowanych danych osobowych, informacja o dokonanym sprostowaniu/uzupełnieniu, ograniczeniu przetwarzania, usunięciu danych osobowych) albo częściowa. Odpowiedź częściowa ma miejsce w sytuacji, gdy żądanie wniosku ma skomplikowany charakter lub zawiera większą liczbę żądań i polega na wyjaśnieniu przyczyn opóźnienia.

W sytuacji, w której Administrator Danych przetwarza duże ilości informacji o osobie, której dane dotyczą, możliwe jest zażądanie od Podmiotu Danych sprecyzowania informacji lub czynności przetwarzania, których dotyczy jej żądanie. Wówczas żądanie sprecyzowania jest traktowane jako odpowiedź częściowa.

W przypadku odpowiedzi częściowej, Pracownik poinformuje Podmiot Danych, że okres na odpowiedź jest przedłużony do łącznie 60 dni od otrzymania wniosku Podmiotu Danych. W takim wypadku, Pracownik musi wysłać ostateczną odpowiedź do Podmiotu Danych w ciągu maksymalnie 21 dni roboczych od daty, w której wysłał do Podmiotu Danych odpowiedź częściową, chyba że Podmiot Danych nie precyzuje wniosku zgodnie z pkt 86. w ciągu 10 dni roboczych od otrzymania żądania sprecyzowania. W ostatnim przypadku ostateczna odpowiedź jest wysyłana w ciągu 5 dni roboczych od otrzymania odpowiedzi Podmiotu Danych.

Jeżeli Podmiot Danych złożył wniosek elektronicznie, wówczas otrzymuje w miarę możliwości odpowiedź za pośrednictwem tego samego kanału. Podmiot Danych może zażądać odpowiedzi inną drogą, wówczas odpowiedź jest udzielana w formie wybranej przez Podmiot Danych.

W przypadku, gdy odpowiedź odnosi się transferu do/dostępu dla danych osobowych dla Podmiotu Danych (np. wniosek o dostęp lub przeniesienie danych osobowych), to dane osobowe będą dostarczone Podmiotowi Danych w formacie elektronicznym, powszechnie używanym i w zrozumiały, łatwy do odczytania sposób. W takim przypadku, Pracownik wskaże w odpowiedzi, jaki zakres danych osobowych jest przekazywany.

Odpowiedź zostanie przekazana Podmiotowi Danych bezpłatnie (z wyjątkiem wniosków, które są woczywisty sposób bezzasadne lub nadmierne.

Pracownik informuje IOD o wyniku każdego kontaktu z Podmiotami Danych.

6. Odmowa uwzględnienia wniosku

Odmowa uwzględnienia wniosku musi być oparta na jednej z okoliczności uzasadniających odmowę, wskazanych szczegółowo w ramach opisu poszczególnych praw Podmiotów Danych.

Jeżeli według oceny Właściciela Biznesowego wniosek nie zasługuje na uwzględnienie, Pracownik zobowiązany jest do przedstawienia projektu odpowiedzi odmownej, z wyjaśnieniem przyczyn IOD w ciągu 2 dni roboczych od daty otrzymania wniosku.

Po otrzymaniu projektu decyzji odmownej IOD dokona przeglądu wniosku i projektu odmowy Właściciela Biznesowego i wyrazi stanowisko w tym zakresie w ciągu 3 dni roboczych.

W odpowiedzi dotyczącej odmowy uwzględnienia wniosku należy podać powody odmowy. Konieczne jest także poinformowanie Podmiotu Danych o możliwości złożenia skargi do Organu Nadzorczego oraz o możliwości dochodzenia roszczeń na drodze cywilnej.

W przypadku, gdy wnioski są ewidentnie nieuzasadnione (tzn. świadczące o nadużywaniu prawa) lub nadmierne (np. z powodu ich powtarzalnego charakteru), Pracownik może podjąć decyzję o:

1) pobraniu rozsądnej opłaty (w tym za dostarczanie danych osobowych w przypadku wniosku o dostęp lub przeniesienie),
2) odmowie uwzględnienia wniosku.

Każda z tych decyzji podlega konsultacji z IOD. W powyższym zakresie obowiązuje swoboda decyzji – odmowa uwzględnienia wniosku nie jest warunkowana odmową/brakiem wniesienia opłaty przez Podmiot Danych. Pracownik może albo podjąć decyzję o wezwaniu do uiszczenia opłaty i wówczas uzależnić dalsze działania od wniesienia opłaty albo podjąć decyzję o odmowie uwzględnienia wniosku bez wzywania do uiszczenia opłaty.

Poprzez rozsądną opłatę należy rozumieć opłatę odzwierciedlającą czas poświęcony na analizę zapytania, projektowanie odpowiedzi, koszt wytworzenia takiej odpowiedzi, koszt doręczenia odpowiedzi (koszty administracyjne oraz uzasadniony koszty pracy), w wysokości, której rozsądnie rzecz oceniając można się spodziewać i która nie stanowi nadmiernego obciążenia dla Podmiotu Danych.

Na Właścicielu Biznesowym spoczywa obowiązek wykazania oczywistej bezzasadności lub nadmiernego charakteru wniosku.

Pracownik zobowiązany jest do przedstawienia projektu odpowiedzi zawierającej żądanie wniesienia opłaty (z wyjaśnieniem przyczyn) IOD drogą mailową w ciągu 2 dni roboczych od daty otrzymania wniosku.

Po otrzymaniu projektu decyzji zawierającej żądanie wniesienia opłaty IOD dokona przeglądu wniosku i projektu odpowiedzi Właściciela Biznesowego, w razie potrzeby konsultując się z Właścicielem Biznesowym. IOD wyraża swoje stanowisko otrzymania projektu odpowiedzi zawierającej żądanie wniesienia opłaty.

Jeżeli w odpowiedzi na żądanie wniesienia opłaty Podmiot Danych nie wniesie opłaty, wówczas wezwanie do uiszczenia opłaty jest ostatnim pismem w sprawie i nie zostaną podjęte dalsze czynności, o czym uprzedza się w treści pisma wzywającego do wniesienia opłaty.

W treści pisma zawierającego żądanie wniesienia opłaty jest wskazany numer rachunku bankowego na który wnosi się opłatę oraz tytuł przelewu. Należy monitorować wpływ wpłaty na konto bankowe.

Po otrzymaniu przez Właściciela Biznesowego informacji jw. biegnie dla niego termin na rozpatrzenie wniosku, który wynosi 5 dni roboczych.

Pracownik informuje IOD o wyniku każdego kontaktu z Podmiotami Danych.

7. Prowadzenie dokumentacji

Pracownik prowadzi szczegółową dokumentację w zakresie obsługi i wyników wniosków, w tym:

1) rejestr wszystkich przychodzących wniosków, w tym ich dat otrzymania; oznacza to konieczność prowadzenia rejestru (np. w formie pliku Excel) uzupełnianego na bieżąco o każdą przychodzącą korespondencję z zakresu realizacji przez Podmioty Danych ich praw. Rejestr zawiera dane wnioskodawców, daty otrzymania żądań od wnioskodawców, numer sprawy, krótki opis żądania/przedmiotu pisma, kategorię żądania (dostęp, sprostowanie, usunięcie itp.).
2) wszystkich kontaktów z Podmiotem Danych w ramach działań podjętych w związku z jego/jej wnioskiem (odpowiedź na wniosek, informacje przekazane Podmiotowi Danych); oznacza to konieczność prowadzenia (np. w formie pliku Excel) rejestru korespondencji wychodzącej z zakresu realizacji przez Podmioty Danych ich praw (wskazanych w niniejszej procedurze) uzupełnianego na bieżąco w zakresie danych takich jak: data nadania odpowiedzi/pisma do Podmiotu Danych, temat pisma, zakres, informacji przekazanych Podmiotowi Danych.

Oba ww. rejestry dotyczą zarówno korespondencji tradycyjnej, jak i mailowej.

IOD prowadzi szczegółową dokumentację swojego zaangażowania w proces realizacji praw Podmiotów Danych (np. dotyczącą wniosków o wsparcie od Właściciela Biznesowego, otrzymanych kopii pism do Podmiotów Danych etc.). Oznacza to konieczność prowadzenia rejestru (np. w formie pliku Excel) wraz załącznikami, uzupełnianego na bieżąco o każdą przychodzącą korespondencję od/do Właściciela Biznesowego, podejmowane kroki, formułowane zalecenia, obserwacje. Rejestr zawiera dane wnioskodawców, daty otrzymania żądań od wnioskodawców, numer sprawy, krótki opis żądania/przedmiotu pisma, kategoria żądania (dostęp, sprostowanie, usunięcie itp.), daty wysłania odpowiedzi, data i sposób realizacji żądania.

Wnioski pochodzące od Podmiotów Danych podlegają przechowywaniu zgodnie z założonym harmonogramem retencji.

Przykład pisemnego wniosku o realizację praw osób.

Białe pola wypełnia wnioskodawca CZYTELNIE.	..... miejscowość i data
..... Oznaczenie Administrator Danych	..... numer wniosku / data wpływu

*WNIOSEK O REALIZACJĘ PRAWA**

- ☐ dostępu do danych
- ☐ sprostowania danych
- ☐ do usunięcia danych ("prawo do bycia zapomnianym")
- ☐ do ograniczenia przetwarzania
- ☐ do przeniesienia danych do innego administratora
- ☐ do sprzeciwu
- ☐ do niepodlegania profilowaniu

Podstawa prawna	*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*

1. Dane osoby wnioskującej

imię/imiona:	.....
Nazwisko:	.....
Adres zamieszkania:	.....
inna dana pozwalająca na identyfikację np. nr dowodu osobistego/PESEL:	.....

2. Informacje identyfikujące osobę wnioskującą w zasobach Administratora Danych osobowych

.....
.....
.....

3. Sposób odbioru danych osobowych przez osobę wnioskującą*

- ☐ wiadomość e-mail
- ☐ doręczenie pocztą**
- ☐ odbiór osobisty

.....
.....
.....

4. Uzasadnienie/uwagi osoby wnioskującej wskazującej na przyczyny składania wniosku

.....
.....
.....
.....
.....
.....
.....
.....

.....
podpis wnioskodawcy

5. Informacje dotyczące wykonania/niewykonania prawa osoby, której dane dotyczą:

* zaznaczyć wybrane

** uzupełnić w przypadku, gdy adres korespondencyjny jest inny niż adres zamieszkania

☐ Administrator przychyla się do wniosku	☐ Administrator odrzuca wniosek
Uzasadnienie decyzji administratora	
.....	
..... *data i podpis ADO*	
zatwierdzenie:	
..... *data i podpis osoby zatwierdzającej*	

1. CEL

Celem niniejszej procedury jest opisanie procesu ustalania i weryfikacji okresu retencji przetwarzanych danych osobowych. Procedura ta jest dostępna dla wszystkich pracowników, a jej znajomość jest obowiązkowa.

2. ODPOWIEDZIALNOŚĆ

Za przygotowanie procesu odpowiedzialny jest Pracownik, natomiast za realizację komórka ds. IT.

W stosunku do każdej czynności przetwarzania danych osobowych, Pracownik zobowiązany jest postępować w następujący sposób:

1) zidentyfikować wszystkie cele przetwarzania danych osobowych i typy (rodzaje) danych osobowych objęte przetwarzaniem, w ramach danej czynności.
2) zdefiniować okres retencji danych osobowych dla każdego z celów przetwarzania i kategorii danych osobowych.
3) weryfikować okresy retencji.

W odniesieniu do spraw będących w toku, jak również wszelkich spraw nieschematycznych czy nietypowych Pracownik zobowiązany jest do indywidualnego określenia terminu retencji, przy zachowaniu zasad: indywidualne określenie terminu retencji następuje w porozumieniu z IOD oraz indywidualne określenie terminu retencji dla indywidualnego procesu dokumentuje w *Harmonogramie okresów retencji danych osobowych*, tworzonym z wykorzystaniem Załącznika 19.

Pracownik zobowiązany jest podejmować decyzje dotyczące ustalenia metody usuwania danych osobowych. Jeżeli nie istnieją okoliczności wstrzymujące usunięcie danych, należy zastosować jedno z poniższych rozwiązań:

1) trwale usunąć dane osobowe. Pracownik jest odpowiedzialny za ustalenie zakresu danych, które powinny zostać usunięte. Jeśli dane osobowe muszą być przechowywane w oparciu o nowe lub zmienione przepisy prawa, powinien uwzględnić te zmiany;
2) dokonać anonimizacji danych osobowych. Gdy usunięcie lub anonimizacja danych związane są z modyfikacją systemu IT, uzgadnia tę czynności z komórką IT. Decyzja odnośnie usunięcia danych osobowych lub anonimizacji jest podjęta (wraz z uzgodnieniami) nie później niż w ciągu 10 dni roboczych od zakończenia okresu retencji. Usuwaniem danych z punktu widzenia technicznego zajmuje się komórka ds. IT.

3. ZAKRES I WARUNKI STOSOWANIA DOKUMENTU

W stosunku do każdej czynności przetwarzania danych osobowych, Pracownik zobowiązany jest postępować w następujący sposób:

1. zidentyfikować wszystkie cele przetwarzania i rodzaje danych objęte przetwarzaniem w ramach danej czynności oraz wskazać je w *Harmonogramie standardowych okresów retencji danych osobowych.*
2. zdefiniować okres retencji danych osobowych dla każdego z celów przetwarzania.

3. weryfikować okresy retencji.

W odniesieniu do spraw będących w toku lub nietypowych, Pracownik zobowiązany jest do indywidualnego określenia terminu retencji z zachowaniem zasady porozumienia z ADO. Indywidualne określenie terminu retencji Pracownik dokumentuje w *Harmonogramie standardowych okresów retencji danych osobowych*. Zobowiązany jest też podejmować decyzje dotyczące ustalenia metody usuwania danych osobowych.

Jeżeli nie zaistnieją okoliczności uzasadniające wstrzymanie się z usunięciem danych, należy zastosować jedno z poniższych rozwiązań:

1. trwale usunąć dane osobowe. Pracownik jest odpowiedzialny za ustalenie zakresu danych, które powinny zostać usunięte. Jeśli dane osobowe muszą być przechowywane w oparciu o nowe lub zmienione przepisy prawa zmieniające wymogi retencji danych, powinien uwzględnić te zmiany;
2. dokonać anonimizacji danych osobowych. Pracownik podejmuje decyzje odnośnie sposobu reakcji na koniec okresu retencji. Gdy usunięcie lub anonimizacja danych związane są z modyfikacją systemu IT, wypełnia wniosek o usunięcie lub anonimizację danych w systemie. Decyzja ta jest podjęta (wraz z wysłaniem wniosku o usunięcie danych) nie później niż w ciągu 10 dni roboczych od zakończenia okresu retencji.
3. Usuwaniem danych z punktu widzenia technicznego zajmuje się komórka ds. IT.
   1) proces technicznego usunięcia danych przez komórkę ds. IT odbywa się bez zbędnej zwłoki.
   2) w przypadku wybranych systemów IT harmonogram technicznego usuwania danych z systemu ustalany jest wspólnie, przez IOD i właściciela systemu ze strony komórki ds. IT. Proces usuwania danych z systemu odbywa się cyklicznie, regularnie, w zaplanowanych ustalonych terminach.
   3) Pracownik jest odpowiedzialny za zagwarantowanie, że wszystkie osoby, które mogą m.in. kopiować, ściągać, przesyłać dane osobowe zostały poinformowane o okresie retencji danych i skasowały dane osobowe ze swoich zasobów.
   4) aby upewnić się, że dane osobowe zostały skasowane przez powyżej wymienione osoby, Pracownik może żądać potwierdzenia usunięcia danych przez te osoby. Przenośne urządzenia lub nośniki danych posiadające dane osobowe powinny zostać zniszczone lub jeżeli jest to możliwe dane trwale usunięte.

Każde usunięcie lub anonimizacja danych osobowych wynikająca z wykonania standardowych okresów retencji danych osobowych jest potwierdzona dowodem.

1) Pracownik (po konsultacji komórką IT) decyduje, w jakim zakresie i przy użyciu jakiej metody dane elektroniczne zostaną usunięte lub zanonimizowane.
2) uzupełniony harmonogram standardowych okresów retencji danych osobowych jest przechowywany (nawet po usunięciu lub zanonimizowaniu) jako potwierdzenie spełnienia wymogu dotyczącego retencji danych.

Okresowa weryfikacja poprawności danych jest dokonywana nie rzadziej niż raz do roku. Pracownik weryfikuje poprawność przetwarzanych danych osobowych, co należy potwierdzić przynajmniej w odniesieniu do następujących kryteriów: aktualność danych osobowych, cel przetwarzania, adekwatność zgód, wstępna analiza ryzyka, harmonogram retencji.

W przypadku zidentyfikowania rozbieżności w wymienionych powyżej obszarach w zakresie przetwarzanych danych w stosunku do stanu faktycznego, Pracownik zobowiązany jest zastosować jedno z poniższych rozwiązań:

a) zaktualizować dane podmiotu, jeśli ma wiedzę na temat aktualnych danych;
b) zadbać o adekwatność posiadanych zgód, zgodnie z polityką ich pozyskiwania;
c) przeprowadzić wstępną analizę ryzyka oraz jeśli zaistnieje potrzeba, ocenę skutków w zakresie ochrony danych;

Wyniki weryfikacji powinny zostać udokumentowane przez Pracownika, a ich poprawność skonsultowana z IOD i odznaczona w dokumentacji. Dokumentacja przechowywana jest przez IOD.

Uwagi:

1. Upływ okresów retencji liczony jest począwszy od końca danego roku kalendarzowego.
2. Raz w roku po upływie okresu retencji należy usunąć niepotrzebne dane.
3. Wszędzie tam, gdzie mowa o okresie n lat, można dodać do 1 roku na wypadek zdarzeń mających miejsce na koniec roku.

Zdarzenia szczególne:

Wydłużające okres retencji: zgłoszenie roszczeń, postępowanie przed organem nadzorczym, postępowanie sądowe – do czasu prawomocnego rozstrzygnięcia sprawy.
Skracające okres retencji: żądanie usunięcia danych (możliwe dalsze przetwarzanie danych osobowych w celach wynikających z przepisów prawa).

4. W przypadku systemów informatycznych obsługujących różne procesy, stosuje się jeden, najdłuższy okres retencji.
5. Propozycje standardowych okresów retencji należy odczytywać w świetle zasady minimalizmu i niezbędności – unikanie powielania przechowywanych tych samych danych w wielu miejscach jednocześnie.
6. Należy mieć na względzie możliwą zmianę przepisów prawa.
7. Można posiłkować się dokumentem JRWA (Jednolity Rzeczowy Wykaz Akt - Dz.U.11.14.67 ROZPORZĄDZENIE PREZESA RADY MINISTRÓW z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych).

Wprowadzenie

Niniejsza procedura określa zasady oraz osoby odpowiedzialne za niszczenie zbiorów danych osobowych utrwalonych w postaci dokumentów papierowych oraz zbiorów zapisanych na nośnikach elektronicznych. Znajomość zasad niszczenia obowiązuje wszystkich pracowników przetwarzających dane osobowe.

I. Zakres

Procedura ta obejmuje realizację procesów niszczenia zbiorów Danych Osobowych.

II. Zakres odpowiedzialności

W realizacji procedury biorą udział:

a) Osoba odpowiedzialna za przetwarzanie danych osobowych;
b) IOD;
c) ASI,
d) Pracownik.

III. Niszczenie zbiorów danych osobowych

Niszczenie dokumentów papierowych oraz nośników elektronicznych jest ściśle powiązane z procesem zarządzania cyklem życia danych osobowych. Proces ten jest nie tylko jednym z elementów polityki bezpieczeństwa, lecz wymaga wdrożenia również w odniesieniu do danych osobowych, dla których brak jest podstawy przetwarzania.

IV. Niszczenie zbiorów danych i jego metody

Dane osobowe mogą być przechowywane przez pracownika na twardym dysku jego komputera służbowego, pamięci flash, na płytach lub dyskach przenośnych, a także w wyniku realizacji standardowych procesów biznesowych Spółki mogą zostać zgromadzone na innych nośnikach (np. taśmy magnetyczne, dyski serwerowe, dyski urządzeń biurowych). Należy zwracać uwagę na zasadę szyfrowania nośników. Podczas wymiany sprzętu, poufność zgromadzonych na nim danych osobowych powinna być w odpowiedni sposób zabezpieczona: poprzez zniszczenie twardego dysku lub trwałe przekształcenie danych do nieczytelnej formy, zachowanie zasady używania szyfrowania w znacznym stopniu zwiększy bezpieczeństwo danych osobowych. Elektroniczne nośniki danych osobowych nie powinny zostać wydane do dalszego użytku lub utylizacji, jeżeli nie zostały wcześniej usunięte wszystkie zawarte na nich dane lub nośnik nie jest zaszyfrowany.

V. Metody niszczenia zbiorów danych osobowych

Dokumenty papierowe powinny zostać zniszczone przy pomocy jednej z (lub kombinacji) poniższych metod:

1) lokalnie dostępna niszczarka – niszczenie dokumentów odbywa się przy pomocy odpowiedniej klasy niszczarek (jeśli możliwe z funkcją cięcia poprzecznego),
2) pojemniki bezpiecznego usuwania – dokumenty są umieszczane przez pracowników w dedykowanych pojemnikach, które są opróżniane z określoną częstotliwością przez wyspecjalizowany podmiot trzeci i przezeń niszczone (o ile ilość i zakres niszczonej dokumentacji wskazuje na pozyskanie tego sposobu niszczenia).

Nośniki elektroniczne (dyski drukarek, dyski kserokopiarek, płyty CD/DVD, dyski komputerowe i serwerowe wszelkich typów, przenośna pamięć typu flash, dyski przenośne, taśmy magnetyczne, karty procesorowe) powinny zostać zniszczone przy pomocy jednej z poniższych metod:

1) nadpisanie nośnika danych – polega nad nadpisywaniu obszarów dysku, w których znajdują się dane przeznaczone do usunięcia;
2) demagnetyzacja – czyli poddanie dysku twardego działaniu silnego impulsu magnetycznego, co skutkować będzie rozmagnesowaniem jego warstwy zapisu, zaleca się stosowanie urządzeń posiadających stosowny certyfikat;
3) fizyczne zniszczenie nośnika, np. łamanie, niszczenie poprzez zmielenie nośnika.

VI. Zasady niszczenia dokumentów papierowych

Dokumenty papierowe podlegające zniszczeniu, to wszystkie bieżące dokumenty nie stanowiące dokumentacji archiwalnej, czyli zbędne wydruki, notatki, niepoprawne dokumenty, zbędne kserokopie, itp.

Zniszczeniu podlega również dokumentacja, dla której nie ma podstaw do dalszego przetwarzania (w tym archiwalna) zgodnie z obowiązującymi procedurami.

Wymagane czynności wykonywane przez Pracowników:

Niszczenie dokumentów papierowych (drobna dokumentacja).
Pracownik samodzielnie niszczy dokumenty w lokalnej niszczarce (jeśli posiada dostęp), dotyczy niewielkiej liczby zbędnych dokumentów (notatki, kserokopie, itp.).
Niszczenie dokumentów papierowych – duży wolumen.
Pracownik umieszcza zbędną dokumentację w pojemniku bezpiecznego usuwania dokumentów (dotyczy dokumentów o znacznym wolumenie, a w przypadku, gdy nie dysponuje lokalną niszczarką – także drobnych dokumentów). Zawartość pojemników jest odbierana z określoną częstotliwością przez podmiot specjalizujący się w niszczeniu dokumentów papierowych. Przy odbiorze pojemników pracownik jest zobowiązany spisać *Protokół przekazania do zniszczenia*, a po zakończeniu procesu niszczenia zadbać o pozyskanie od firmy zewnętrznej *Protokołu zniszczenia.*
Niszczenie dokumentów papierowych – dokumentacja archiwalna.
Właściciel Biznesowy przeprowadza analizę okresów zbiorów danych osobowych i po zidentyfikowaniu papierowych zbiorów, informuje pracowników o konieczności zniszczenia danych oraz przekazuje zlecenie zniszczenia dokumentacji do firmy archiwizacyjnej (jeśli dotyczy). Pracownik przekazuje wyszczególnienie dokumentów do zniszczenia do firmy archiwizacyjnej która samodzielnie niszczy dokumenty lub przekazuje do wyspecjalizowanego podmiotu wskazanego przez Spółkę. Pracownik może być obecny przy procesie niszczenia, jest odpowiedzialny za archiwizację Protokołu zniszczenia. Wymagana dokumentacja: Harmonogram okresów retencji, Specyfikacja dot. danych podlegających zniszczeniu, Protokół zniszczenia

VII. Zasady niszczenia elektronicznych nośników danych

Niszczeniu podlegają te nośniki, dla których minął okres ich ważności, nie przewiduje się ich dalszego użytkowania lub istnieje prawdopodobieństwo, że dalsze ich użytkowanie może nie spełniać wymogów bezpieczeństwa przechowywania informacji.

Wszyscy pracownicy są zobowiązani przekazywać wszelkie nośniki danych do ASI, który decyduje o sposobie dalszego procedowania z określonym nośnikiem, w tym niszczeniu przez firmę zewnętrzną.

Wymagane czynności wykonywane przez Pracowników:

Niszczenie nośników elektronicznych – płyty.
Pracownicy dostarczają płyty niepotrzebne, uszkodzone oraz takie, które zawierają dane, dla których brak jest podstaw przetwarzania do IT. Pracownik IT na bieżąco niszczy płyty w specjalistycznej niszczarce. Dokumentacja: Zapis w dzienniku systemu.
Niszczenie nośników elektronicznych – taśmy magnetyczne.
IT ocenia taśmy, które są niepotrzebne, uszkodzone lub zawierają dane, dla których brak jest podstaw przetwarzania do IT. Pracownik IT na bieżąco niszczy taśmy poprzez wyciągnięcie ich z obudowy i rozcięcie na wiele drobnych części lub korzysta z usług firmy zewnętrznej. Wymagana dokumentacja: Wpis w dzienniku systemu lub Protokół przekazania do zniszczenia i zniszczenia.
Niszczenie nośników elektronicznych – pozostałe (dyski, pamięć flash, karty procesorowe, inne).
Pracownicy dostarczają do IT wszelkie nośniki danych, dla których minął okres ich ważności, nie przewiduje się ich dalszego użytkowania lub istnieje prawdopodobieństwo, że dalsze ich użytkowanie może nie spełniać wymogów bezpieczeństwa przechowywania informacji. IT przechowuje nośniki w dedykowanym pojemniku. Wyspecjalizowany podmiot odbiera ze Spółki nośniki przeznaczone do zniszczenia. W procesie uczestniczy osoba zarządzająca IT, który jest odpowiedzialna za sporządzenie *Protokołu przekazania do zniszczenia.* Przedstawiciel Spółki może być obecny przy procesie niszczenia w siedzibie firmy zewnętrznej. Po zakończeniu procesu niszczenia sporządzany jest *Protokół zniszczenia.*

VIII. Niszczenie danych w dokumentach elektronicznych,

Niszczenie danych w bazach danych, plikach powinno odbywać się zgodnie ze stanem wiedzy, w sposób adekwatny do niszczonego zasobu. Wskazane jest, o ile to możliwe wykorzystanie specjalizowanego oprogramowania. Proces niszczenia powinien być bezwzględnie nieodwracalny. Każdorazowo metodę usuwania danych proponuje ASI a zatwierdza Administrator. Niszczenie danych elektronicznych doprecyzowane jest w Załączniku nr 3.

IX. Załączniki:

Załącznik nr 1. Protokół z przekazania do zniszczenia

Załącznik nr 2. Protokół ze zniszczenia

Załącznik nr 1 „Protokół z przekazania do zniszczenia"

Protokół przekazania do zniszczenia

Niniejszym przekazuję:

pliki elektroniczne na nośniku o numerze identyfikacyjnym ..... /

dokumentacje papierową .....
[CD, DVD, dysk przenośny, pendrive, dyskietka, inne .....]

Zawierające:

.....

[dane handlowe, dane osobowe, baza danych systemu ....., zestawienie, inne.....]

Celem zniszczenia.

.....

.....

Data i podpis odbierającego

Data i podpis przekazującego

Załącznik nr 2 „Protokół ze zniszczenia"

PROTOKÓŁ ZNISZCZENIA

W dniu ..... komisja w składzie:

.....
(imię i nazwisko, zajmowane stanowisko/pełniona funkcja)

.....
(imię i nazwisko, zajmowane stanowisko/pełniona funkcja)

.....
(imię i nazwisko, zajmowane stanowisko/pełniona funkcja)

dokonała trwałego zniszczenia następujących rzeczy:

L.p..	Co zostało zniszczone	Przyczyny zniszczenia
1		

Zniszczenia dokonano poprzez

.....

Podpisy członków komisji:

1. .....

2. .....

Dostosowanie monitoringu gminnego do wymagań RODO.

Wszystkie procesy dotyczące monitoringu, podlegają rygorom rozporządzenia 2016/679 RODO, które bezpośrednio w art. 35 wspomina o systematycznym monitorowaniu na dużą skalę miejsc dostępnych publicznie, u.o.d.o. oraz ustaw szczególnych i aktów wykonawczych. Regulują one uprawnienia i obowiązki podmiotów mogących prowadzić obserwację przede wszystkim miejsc publicznych, osób i mienia w celu zapewniania bezpieczeństwa.
Odnosząc się do zakresu danych osobowych przetwarzanych przez monitoring wizyjny właściwym jest wskazywanie w szczególności wizerunków, cech szczególnych osób i numerów identyfikacyjnych (np. numery tablic rejestracyjnych i numerów bocznych pojazdów). W przypadku monitoringu wizyjnego będą to operacje polegające w szczególności na zapisywaniu, przeglądaniu, udostępnianiu i usuwaniu nagrań zarejestrowanych zdarzeń i osób niezależnie od charakteru nośnika, w którym są przechowywane (dyski twarde systemu, nagrania zapisane w pamięci urządzenia umożliwiającego zdalny dostęp - smartfon, komputery przenośne itp.). Mając na uwadze, że nagrania mogą być analizowane klatka po klatce i przy użyciu specjalnych metod technicznych (automatyczna analiza obrazu) wykorzystane do identyfikacji osób obserwowanych, tylko takie systemy monitorowania będą przetwarzały dane biometryczne w rozumieniu art. 9 ust. 1 RODO. Tego typu operacje wymagać będą wyczerpujących podstaw prawnych oraz wypełnienia dodatkowych obowiązków związanych z przetwarzaniem szczególnych kategorii danych osobowych. Obejmuje to w szczególności dokonanie oceny skutków dla ochrony danych na podstawie art. 35 ust. 3 lit. b RODO obok wymaganej dla systemów monitoringu oceny na podstawie lit. c tego samego przepisu.

Zasady przetwarzania danych osobowych

Główne zasady postępowania przy przetwarzaniu danych osobowych wyznacza art. 5 ust. 1 RODO, ujmując je w formę podstawowych obowiązków administratora. Z jego treści wynika, że dane osobowe muszą być:
a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (**zgodność z prawem, rzetelność i przejrzystość**);
b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami (**ograniczenie celu**);
c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (**minimalizacji danych**);
d) prawidłowe i w razie potrzeby uaktualniane, a dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, muszą być niezwłocznie usunięte lub sprostowane (**prawidłowość**);
e) przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane (**ograniczenie przechowywania**);
f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową
utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (**integralność i poufność**).

Osoba, której dane dotyczą - osoba obserwowana
Zidentyfikowana lub możliwa do zidentyfikowania osoba fizyczna, której dane zostaną zebrane poprzez system monitoringu wizyjnego, może korzystać z praw ujętych w rozdziale III rozporządzenia. Mając na uwadze specyfikę wideomonitoringu, należy stwierdzić, że realizacja uprawnień kontrolnych osoby obserwowanej może się wiązać z koniecznością przedstawienia przez nią informacji o sytuacjach, w których mogła znaleźć się w obszarze działania systemu monitoringu. Może to obejmować okresy czasu czy też sytuacje, w których uczestniczyła taka osoba, szczegóły jej ubioru itp. Zgodnie z ostatnim zdaniem motywu 63, jeżeli administrator przetwarza duże ilości informacji o osobie, której dane dotyczą, powinien on mieć możliwość zażądania, przed podaniem informacji, by osoba, której dane dotyczą, sprecyzowała informacje lub czynności przetwarzania, których dotyczy jej żądanie. Jeżeli przepisy szczególne nie stanowią inaczej, odpowiedź na zapytania osoby obserwowanej powinna zostać udzielona bez zbędnej zwłoki, najpóźniej w ciągu miesiąca.

Wizerunek jako dobro osobiste.

Bez względu na przypisanie zapisu wizerunku (np. zapisu pochodzącego z monitoringu miejskiego) do kategorii danych osobowych, należy zauważyć, że wizerunek jest również **samodzielnym dobrem osobistym człowieka (art. 23 ustawy z 23 kwietnia 1964 r. - Kodeks cywilny)**. Sądy powszechne zwracają przy tym uwagę, że wizerunek jako dobro osobiste powinien być rozumiany jako pewien obraz fizyczny.

Realizacja zasad przetwarzania danych osobowych należy do obowiązków **administratora**, którym zgodnie z art. 4 pkt 7 rozporządzenia jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, samodzielnie lub wspólnie z innymi ustalający cele i sposoby przetwarzania danych osobowych.
Administratorem danych osób obserwowanych (operator systemu monitoringu) jest podmiot, który podejmuje decyzje o instalacji, celach i obszarze objętym systemem monitoringu będącym w jego dyspozycji. Może on działać przez osoby kierujące i reprezentujące go na zewnątrz, jak np. zarząd spółki, dyrektor szkoły itd. Funkcjonariusze ci zobowiązani są zapewnić w kierowanej przez siebie jednostce organizacyjnej zgodne z prawem przetwarzanie danych osobowych oraz ponoszą odpowiedzialność za działania wszystkich osób upoważnionych do przetwarzania danych.

Podejmując decyzję o wprowadzeniu monitoringu, administrator musi pamiętać o przeprowadzeniu **oceny skutków dla ochrony danych (DPIA).**

Istotne znaczenie ma realizacja wobec osoby obserwowanej obowiązku informacyjnego ujętego w art. 13 RODO. Musi on być, zgodnie z art. 12 rozporządzenia, realizowany w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część z wymienianych powyżej przepisów szczególnych wskazuje dodatkowo znaki lub ogłoszenia dźwiękowe, którymi należy oznaczyć pomieszczenia i teren monitorowany (w/w przepisy Kodeksu pracy i Prawa oświatowego). Pełna informacja o monitoringu, obejmująca wszystkie wymogi art. 13 RODO, powinna być dostępna w miejscu monitorowanym, np. na tablicach albo w formie dokumentu dostępnego u przedstawiciela administratora, czyli możliwa jest

realizacja obowiązku informacyjnego poprzez podanie informacji podstawowych i uzupełnienie ich w kolejnych warstwach informacyjnych. Znaki informujące o stosowaniu monitoringu powinny być dostępne przed wejściem w obszar obserwowany.

W przypadku wniosków o dostęp do nagrań kierowanych do administratora przez organy publiczne i służby porządkowe, powinny być one związane z realizacją zadań tych podmiotów i zgodne z obowiązującymi je zasadami pozyskiwania danych osobowych. W obu powyższych sytuacjach przypadki udostępnienia powinny być prawidłowo udokumentowane. W myśl zasady rozliczalności, jest to konieczne, by administrator mógł wykazać, że przetwarzał dane zgodnie z obowiązującym prawem.

Administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa uwzględniający stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania, a także ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze. Obejmuje to wymogi ujęte w sekcji II rozdziału 4 RODO - Bezpieczeństwo danych osobowych.
Administrator prowadzi dokumentację opisującą sposób przetwarzania danych oraz zastosowane środki techniczne i organizacyjne, a także ewidencję osób upoważnionych do ich przetwarzania. Do przetwarzania danych, o ile tak zdecyduje ich administrator, mogą być dopuszczone wyłącznie osoby działające z upoważnienia administratora lub podmiotu przetwarzającego i przetwarzają je wyłącznie na polecenie administratora.

W sytuacji, gdy przepisy szczególne nie określają wymogów co do środków technicznych i organizacyjnych, to administrator ma swobodę w tej materii i odpowiada za wykazanie, że są one wystarczające.

Tym samym proponuję wdrożyć następujące elementy uwzględniające odpowiedzialność:

1. Instrukcję zarządzania systemem monitoringu uwzględniającą m.in.:

Obszar który objęty jest monitoringiem wizyjnym jest oznakowany w sposób jednoznaczny.

Administratorem danych jest: .....

Osobą odpowiedzialną za weryfikację prawidłowości oznakowania obszaru jest: .....

Obszar monitoringu obejmuje: .....

Osobą odpowiedzialną za aspekt techniczny monitoringu jest: .....

Podstawy prawne

- art. 1 ust. 1, art. 5 ust. 2 ustawy z 6 września 2001 r. o dostępie do informacji publicznej (j.t. Dz.U. z 2016 r. poz. 1764);
-Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 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 RODO);
- Ustawa o ochronie danych osobowych (Dz.U. z 2018 nr 1000);
- art. 23 ustawy z 23 kwietnia 1964 r. - Kodeks cywilny (j.t. Dz.U. z 2017 r. poz. 459; ost. zm. Dz.U. z 2017 r. poz. 1132);
- Art. 9a ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2018 r. poz. 994 i 1000);
- Art. 11 ustawy z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych (Dz. U. z 2017 r. poz. 1160 z późn. zm.)
- Art. 222 ustawy z dnia 26 czerwca 1974 r. - Kodeks pracy (Dz. U. z 2018 r. poz. 917 i 1000);
- Art. 15 i 19 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2017 r. poz. 2067 z późn. zm.);
- Art. 20g ustawy z dnia 21 marca 1985 r. o drogach publicznych (Dz. U. z 2017 r. poz. 2222 z późn. zm.);
- Art. 157 ustawy z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (Dz. U. z 2018 r. poz. 155 z późn. zm.);
- Art. 147 ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz. U. z 2017 r. poz. 1904 z późn. zm.).

2. Zasady dokumentowania

Administrator systemu wizyjnego dokumentuje swoją działalność w dzienniku systemu przechowanym wraz z systemem monitoringu. Zawarta powinna być w nim informacja zawierająca: datę i godzinę czynności, rodzaj czynności (np. przegląd techniczny systemu, przegląd danych wizyjnych, prezentacja danych

wizyjnych, kopiowanie danych wizyjnych, usuwanie danych starszych niż 90 dni)

W przypadku prezentowania danych wizyjnych niezbędny jest szczegółowy opis uwzględniający dane osoby dopuszczonej do informacji, cel uzyskania dostępu wraz z podstawą prawną oraz jej podpis. W przypadku kopiowania danych niezbędny jest dokument potwierdzający zabezpieczenia danych.

Zgodnie z prawem dostęp do danych posiada Administrator Danych oraz organy z mocy prawa (Policja, Prokuratura, Sąd). Organy te w przypadku żądania otrzymania danych pozostawiają dokument o zabezpieczeniu dowodów.

Niedopuszczalne jest przeglądanie danych monitoringu wizyjnego w celach prywatnych *(W przypadku uznania zapisu monitoringu wizyjnego za informację publiczną wydaje się, że w większości przypadków kopia takiego zapisu nie będzie mogła zostać wydana ze względu na potrzebę ochrony prywatności osób fizycznych. Organ powinien odmówić udostępnienia na podstawie art. 5 ust. 2 u.d.i.p.)*