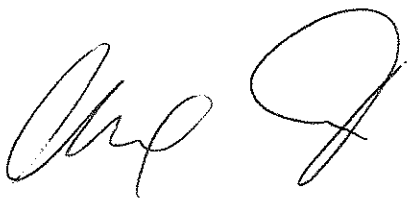
BizTech Konsulting SA

POLITYKA BEZPIECZEŃSTWA



Zatwierdził:

Data zatwierdzenia:

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 (tymczasowo lub długoterminowo), odbywającą staż lub praktyki studenckie.

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

Dane osobowe są przetwarzane w BizTech Konsulting SA 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*). 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) 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.),

3) Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922, z 2018 r. poz. 138.ze zm.).

Używane skróty.

1. **Administrator danych, ADO** – Zarząd Konsulting SA (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 BizTech Konsulting SA 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, generowane na przykład przez etykiety Radio-Frequency Identification (RFID). 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

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. zbiorowej – wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych i aktywnie
- 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 BizTech Konsulting SA.
- 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 Izbie 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 BizTech Konsulting SA znajdującej się w Warszawie przy ulicy Wolność 3A. 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. Upoważnienie do przetwarzania danych.*

- 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.* BizTech Konsulting SA 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 powstaną dokumenty *Protokół szacowania ryzyka dla dokumentów tradycyjnych (Załącznik nr 12)* oraz *Protokół szacowania ryzyka dla dokumentów elektronicznych (Załącznik nr 13)* które powinny być cyklicznie sporządzane, nie rzadziej niż raz w roku oraz przy każdej zmianie czynników powodujących zagrożenie. Możliwe jest wykorzystanie innych metod szacowania. Osobą odpowiedzialną jest ADO lub osoba przez niego wyznaczona. ADO ma prawo wyznaczyć Pełnomocnika ds. danych osobowych a wzór upoważnienia zawarty jest w dokumencie *Upoważnienie dla pełnomocnika ds. danych osobowych (Załącznik nr 14)* lub Inspektora Ochrony Danych

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
- określenie przedmiotu 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.*

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 5. Inwentaryzacja zasobów informacyjnych.xlsx
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.xlsx
Załącznik nr 10a. Wzór rejestru wszystkich kategorii czynności przetwarzania.
Załącznik nr 11. Ogólne szacowanie ryzyka.
Załącznik nr 12. Protokół szacowania ryzyka dla dokumentów tradycyjnych.
Załącznik nr 13.Protokół szacowania ryzyka dla dokumentów elektronicznych.
Załącznik nr 14. Upoważnienie dla pełnomocnika ds. danych osobowych.
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.