Powiatowy Zespół
Szkół nr 2
im. K. Miarki
w Pszczynie

Dokument przyjęty Zarządzeniem Dyrektora
PZS2 z dnia 30.08.2018 r.

Załącznik do Zarządzenia nr 7/17/18

POLITYKA BEZPIECZEŃSTWA

2018

POLITYKA BEZPIECZEŃSTWA
Powiatowego Zespołu Szkół nr 2 im. K. Miarki w Pszczynie

Cel i zakres polityki bezpieczeństwa

Powiatowy Zespół Szkół nr 2 im. K. Miarki w Pszczynie, jako administrator danych osobowych, wyraża pełne zaangażowanie dla zapewnienia bezpieczeństwa przetwarzanych przez placówkę danych osobowych oraz wyraża pełne wsparcie dla przedsięwzięć technicznych i organizacyjnych związanych z ochroną danych osobowych oraz poprawą bezpieczeństwa danych.

Niniejsza Polityka Bezpieczeństwa ma w szczególności określić i opisać:

- podstawowe zasady bezpieczeństwa i zarządzania, aby ułatwić i odpowiednio zabezpieczyć przetwarzanie danych osobowych w placówce;
- postępowanie z wszystkimi danymi osobowymi przetwarzanymi w placówce, niezależnie od formy ich przetwarzania (w formie papierowej – tradycyjnej, czy elektronicznej);
- umożliwić przetwarzanie danych osobowych w placówce w zgodzie z prawem oraz w sposób uniemożliwiający nieupoważniony dostęp do danych czy narażający dane na uszkodzenie, zniszczenie lub nieuprawnioną ich modyfikację.

Polityka Bezpieczeństwa jest stosowana przez wszystkie komórki organizacyjne placówki oraz przez wszystkie osoby zatrudnione w ramach wszystkich czynności przetwarzania podejmowanych w placówce.

Z uwagi na nieustannie zmieniające się zagrożenia przetwarzania danych osobowych, w tym w szczególności mając na uwadze rozwój technologiczny, placówka podkreśla, że niniejszy dokument będzie w ramach potrzeby poddawany niezbędnym aktualizacjom, a wprowadzone na jego procedury będą dopasowywane do potrzeb i warunków pracy oraz pracowników przy zachowaniu niezbędnych poziomów bezpieczeństwa przetwarzanych danych osobowych.

Na podstawie i w celu realizacji powyższych Powiatowy Zespół Szkół nr 2 im. K. Miarki w Pszczynie przyjmuje Politykę Bezpieczeństwa o następującej treści:

§1
[Definicje]

Definicje stosowane w niniejszej Politycy Bezpieczeństwa znajdują zastosowanie także w pozostałych dokumentach i załącznikach do Polityki Bezpieczeństwa, tworzących razem szeroko rozumianą Politykę Ochrony Danych Osobowych Powiatowego Zespołu Szkół nr 2 im. K. Miarki w Pszczynie.

1. **Administrator** lub **Placówka** – Powiatowy Zespół Szkół nr 2 im. K. Miarki w

Pszczynie, jako podmiot decydujący o celach i środkach przetwarzania danych osobowych, odpowiedzialny za nadzór nad przestrzeganiem zasad ochrony danych osobowych w jednostce oraz wykonujący zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym, zwany dalej PZS2.

2. **Inspektor Ochrony Danych Osobowych** – osoba odpowiedzialna za kontrolowanie i opiniowanie procesów przetwarzania oraz przestrzegania postanowień niniejszej Polityki przez Administratora.
3. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
4. **Przetwarzanie danych** – jakiekolwiek operacje wykonywane na Danych osobowych, w szczególności takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie w formie tradycyjnej oraz w systemach informatycznych.
5. **Forma tradycyjna** – sposób utrwalenia danych osobowych lub informacji w wersji papierowej.
6. **System informatyczny** – wszystkie urządzenia, programy i usługi informatyczne wykorzystywane przy okazji przetwarzania danych osobowych w PZS2.
7. **Użytkownik** – osoba upoważniona przez Administratora do przetwarzania danych osobowych.
8. **Uwierzytelnianie** – działanie, którego celem jest potwierdzenie (weryfikacja) deklarowanej tożsamości osoby.
9. **Identyfikator** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
10. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi.
11. **Usuwanie danych** – zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwala na ustalenie tożsamości osoby, której dane dotyczyły.
12. **Pseudonimizacja danych** – modyfikacja danych osobowych, która nie pozwala na odczytanie danych osobowych bez dostępu do odpowiedniego klucza (np. nadanie numerów określonym dzieciom).
13. **Osoby trzecia** – osoba spoza struktury organizacyjnej PZS2, zależnie od kontekstu mogą to być interesanci, kontrahenci, uczniowie lub rodzice.

§2
[Zasady przetwarzania danych osobowych]

1. Administrator zapewnia bezpieczeństwo przetwarzanych w placówce danych osobowych poprzez przywiązanie szczególnej uwagi do stosowania i wykorzystywania, w przypadku każdego rodzaju przetwarzania danych osobowych w placówce, niżej wyrażonych zasad.
2. W ramach realizowanych obowiązków i wykonywanych zadań należy przede wszystkim stosować Zasady Podstawowe (ust. 3), jednakże w przypadku nabrania wątpliwości jak zachować się w określonej sytuacji lub natrafienia na sytuację

nieobjętą procedurą (brak wzorów, brak formularzy, brak szkolenia) użytkownik powinien stosować się do Zasad Uzupełniających (ust. 4) i w razie możliwości konsultować swoje postępowanie z Dyrektorem Szkoły i/lub Inspektorem Ochrony Danych Osobowych, jednocześnie w każdej sytuacji z odpowiednią troską i poszanowaniem odnosząc się do przetwarzanych danych osobowych.

3. Zasady Podstawowe tworzy:
    a. zgodność z procedurami – każdy użytkownik w ramach wykonywanych obowiązków powinien postępować zgodnie z przyjętymi w placówce wzorami i procedurami
    b. integralność i poufność – w trakcie pracy z danymi osobowymi musimy zapewnić najwyższy standard ochrony i bezpieczeństwa wszystkich danych osobowych, z którymi mamy do czynienia; niezbędne jest uzmysłowienie sobie wartości tych danych dla osoby, która w zaufaniu nam je przekazała; postępujmy z przetwarzanymi danymi osobowymi z najwyższym szacunkiem (tak jak chcielibyśmy, żeby inni traktowali nasze dane osobowe).
    c. przejrzystość – we wszelkich kontaktach z osobą, której dane dotyczą należy traktować ją z najwyższym szacunkiem starając się odpowiedzieć na wszystkie jej pytanie związane z przetwarzaniem jej danych osobowych przez placówkę, udzielając odpowiedzi w sposób na tyle prosty i zrozumiały, aby była w stanie zaspokoić swoje potrzeby; w przypadku wątpliwości co do legalności udzielenia odpowiedzi na niektóre pytania czy braku dostatecznych informacji należy pomóc takiej osobie nawiązać kontakt z Inspektorem Ochrony Danych Osobowych.
4. Zasady Uzupełniające tworzy:
    a. ograniczenie celu – przetwarzanie danych osobowych może odbywać się tylko i wyłącznie w ramach określonego wcześniej celu, dlatego niezbędne w pierwszej kolejności (przed podjęciem przetwarzania) jest określenie celu, dla którego go dokonujemy (po co zbieramy dane? dlaczego je komuś przekazujemy?).
    b. zgodność z prawem i rzetelność – dane osobowe mogą być przetwarzane jedynie w sytuacji, gdy posiadamy odpowiednią podstawę prawną dla ich przetwarzania (zgoda, umowa, obowiązek prawny, ochrona żywotnych interesów osoby, wykonanie zadań realizowanych w interesie publicznym lub w ramach władzy publicznej) i jeżeli planowane przez nas przetwarzanie jest uczciwe (nie wykorzystuje drugiej strony, nie nadużywa naszej pozycji w relacji z tą osobą), dlatego też zaraz po ustaleniu celu przetwarzania danych osobowych musimy ustalić czy mamy do tego prawo (podstawę prawną).
    c. minimalizacja danych – rozpoczynając przetwarzanie musimy określić ile danych osobowych potrzebujemy przetwarzać, aby być w stanie zrealizować pierwotnie założony cel; nigdy nie zbieramy więcej danych niż jest to nam potrzebne; w ramach pracy placówki zbieramy tylko tyle danych ile jest niezbędne, żeby móc wykonać określoną czynność (nigdy więcej, nigdy „na zapas”).
    d. prawidłowość – musimy przetwarzać dane prawidłowe, a więc musimy

umożliwić osobie, której dane dotyczą wskazanie nam aktualnych danych, a dane niepoprawne niezwłocznie usuwamy lub modyfikujemy.

e. ograniczenie przechowywania – przetwarzając dane osobowe musimy ustalić przez jaki rozsądny okres czasu będą nam one potrzebne, niezwłocznie gdy dane nie będą już dłużej potrzebne, a prawo nie mówi inaczej, jesteśmy zmuszeni usunąć dane osobowe.

5. Podstawowe informacje w zakresie wyżej wymienionych zasad przetwarzania danych osobowych oraz ogólnych zasad postępowania Administrator opisał w przystępnych infografikach, które stanowią **załącznik nr 1** do Polityki Bezpieczeństwa i które zostaną udostępnione pracownikom celem zapewnienia spokojniejszej, zgodnej z procedurami i bezpiecznej pracy z danymi osobowymi przetwarzanymi w ramach wykonywanych obowiązków.

§3
[Relacje z podmiotami danych]

1. Realizując zasadę przejrzystości, wyszczególnionej w §2 Polityki Bezpieczeństwa, Administrator podkreśla niezwykle istotną wagę prostej, dostosowanej do odbiorcy, formy komunikacji z osobami, których dane osobowe przetwarzane są przez Administratora.
2. Każde zgłoszenie żądania realizacji prawa związanego z ochroną danych osobowych wymaga niezwłocznego zawiadomienia Inspektora Ochrony Danych lub Dyrektora Szkoły (czy innych osób przez niego wyznaczonych).
3. Zgodnie z art. 13 RODO Administrator realizuje obowiązek informacyjny wobec podmiotów danych w momencie pozyskiwania od nich tych danych.
4. Wzór obowiązku informacyjnego, o którym mowa w ust. 2 niniejszego paragrafu, stanowi **załącznik nr 2** do Polityki Bezpieczeństwa.
5. Administrator zgodnie z art. 14 RODO, jeżeli taka sytuacja będzie miała miejsce, realizuje obowiązek informacyjny również względem podmiotów danych, których dane uzyskał z innych źródeł niż bezpośrednio od podmiotu danych.
6. W przypadku, gdy podmioty danych posiadają już informacje wchodzące w zakres obowiązków informacyjnych, o których mowa ust. 2 i 4 niniejszego paragrafu, Administrator zwolniony jest z obowiązku udzielania tych informacji.

§4
[System informatyczny]

Sposób zabezpieczenia, zarządzania oraz zasady przetwarzania danych w systemie informatycznym reguluje Instrukcja Zarządzania Systemem Informatycznym stanowiąca **załącznik nr 3** do Polityki Bezpieczeństwa.

§5
[Inspektor Ochrony Danych Osobowych]

1. Administrator wyznacza Inspektora Ochrony Danych Osobowych w celu

nadzorowania i przestrzegania zasad ochrony danych osobowych oraz procesów przetwarzania danych osobowych w placówce, w szczególności z uwzględnieniem wewnętrznych procedur (w tym niniejszej Polityki Bezpieczeństwa) oraz regulujących materię danych osobowych aktów prawnych, tj. przede wszystkim Rozporządzenie Parlamentu Europejskiego i Rady Europejskiej 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 (Ogólnego Rozporządzenia o Ochronie Danych - RODO) oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

2. Szczegółowy wykaz obowiązków Inspektora Ochrony Danych Osobowych określony jest w **załączniku nr 4** do Polityki Bezpieczeństwa.

§6
[Realizacja Polityki Bezpieczeństwa]

1. Administrator celem skutecznej realizacji Polityki Bezpieczeństwa zapewnia i wprowadza:
    a. odpowiednie zabezpieczenia, zarówno w wymiarze fizycznym, technicznym, jak i organizacyjnym;
    b. szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony;
    c. kontrolę i nadzór i wsparcie nad przetwarzaniem danych osobowych ze strony Inspektora Ochrony Danych Osobowych;
    d. kontrolę i nadzór i wsparcie nad przetwarzaniem danych osobowych ze strony Dyrektora Szkoły i osób przez niego wyznaczonych;
    e. monitorowanie i dostosowywanie zastosowanych środków ochrony;
    f. ciągłe śledzenie zmieniających się zagrożeń wewnętrznych i zewnętrznych, wraz z uwzględnieniem zmieniającego się prawa;
    g. kontrolę i nadzór nad przetwarzaniem danych osobowych przez podmioty trzecie, którym dane zostały udostępnione lub powierzone;
    h. wsłuchiwanie się w zalecenia i sugestie Inspektora Ochrony Danych Osobowych oraz pozostałego personelu, pracowników i kadry pedagogicznej.
2. Monitorowanie zastosowanych środków ochrony obejmuje m.in. działania użytkowników, przypadki naruszania zasad dostępu do danych, zapewnienie integralności plików czy ochronę przed sieciowymi atakami zewnętrznymi oraz wewnętrznymi.

§7
[Obszar przetwarzania]

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe określa niejawny **załącznik nr 5** do Polityki Bezpieczeństwa.

§8
[Zbierane dane osobowe i zakres ich przetwarzania]

1. Administrator nie podejmuje się czynności przetwarzania, które mogłyby się wiązać z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka dla praw i wolności osób.
2. W przypadku działania, dla którego można przypuszczać wystąpienie wysokiego ryzyka dla praw i wolności osób, o którym mowa w ust. 1, Użytkownik informuje o takim działaniu lub planie działania Administratora, który analizuje zagrożenia związane z takim działaniem wykonując, w szczególności czynności określone w art. 35 i nast. RODO.
3. W przypadku planowania nowych czynności przetwarzania Administrator dokonuje analizy ich skutków dla ochrony danych osobowych, biorąc pod uwagę kwestię ich odpowiedniej ochrony i zabezpieczenia już w fazie projektowania tych czynności.
4. Zgodnie z art. 30 RODO Administrator prowadzi rejestr czynności przetwarzania oraz – gdy ma to zastosowanie - rejestr kategorii przetwarzania.
5. Rejestry wskazane w §7 ust. 4 Polityki Bezpieczeństwa prowadzone są przez Administratora w formie elektronicznej i przechowywane są na komputerze Administratora w odpowiednio zabezpieczony sposób.
6. Wszystkie czynności podejmowane w ramach pracy Administratora, które zawierają dane osobowe podejmuje się przy uwzględnieniu reguły wynikających z niniejszej Polityki, a w przypadku działania niestandardowego lub przypuszczalnie niosącego na sobie większe ryzyko np. udostępnienia danych, zgubienia ich czy ich zniszczenia, Użytkownik w pierwszej kolejności informuje i konsultuje podjęcie takiego działania z Administratorem.
7. Wykaz wskazaniem programów wykorzystywanych do przetwarzania danych osobowych określa **załącznik nr 6** do Polityki Bezpieczeństwa.

§9
[Upoważnienie do przetwarzania danych osobowych]

1. Do przetwarzania danych mogą być zostać dopuszczone wyłącznie osoby posiadające odpowiednie upoważnienie nadane przez Administratora, zgodnie ze wzorem, stanowiącym **załącznik nr 7** do Polityki Bezpieczeństwa.
2. Pracownik jest zobowiązany zapoznać się z Polityką Bezpieczeństwa i wszystkimi jej załącznikami w zakresie wskazanym przez Administratora, a ponadto Administrator jest zobowiązany udostępnić Politykę Bezpieczeństwa w ustalonym wcześniej zakresie na każde żądanie pracownika.
3. Każdy pracownik jest zobowiązany do zapoznania się, zaakceptowania i stosowania postanowień Polityki Bezpieczeństwa.
4. Każdy pracownik upoważniony do przetwarzania danych osobowych w placówce zobowiązany jest podpisać odpowiednie oświadczenie o zapoznaniu się z zasadami przetwarzania danych osobowych w placówce i zobowiązującego upoważnionego do zachowania poufności przetwarzanych danych osobowych.
5. Wzór oświadczenia, o którym mowa w ust. 4 niniejszego paragrafu, stanowi

załącznik nr 8 do Polityki Bezpieczeństwa.

6. Pracownicy ponad zapisy wynikające z obowiązujących przepisów oraz treści podpisanego oświadczenia o zachowaniu pozyskanych informacji w tajemnicy, zobowiązani są do:
    a. ścisłego przestrzegania zakresu nadanego upoważnienia;
    b. zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia u Administratora;
    c. niezwłocznego zgłaszania wszystkich incydentów (czy innych zdarzeń), mogących stanowić naruszenie bezpieczeństwa danych, a będących niewłaściwym funkcjonowaniem Administratora, bezpośrednio do Administratora.
7. Naruszenie przyjętych w placówce zasad i przepisów ochrony danych osobowych może stanowić ciężkie naruszenie podstawowych obowiązków pracowniczych.
8. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony danych osobowych uważa się w szczególności:
    a. naruszenie bezpieczeństwa systemów informatycznych (m.in. pozostawienie otwartych komputerów bez opieki, niezmienianie lub przyjęcie hasła poniżej ustalonych u Administratora standardów, dzielenie się swoimi loginami i hasłami, logowanie się do systemów sieciowych przez niezabezpieczone sieci publiczne, otwieranie podejrzanych załączników);
    b. udostępnianie lub umożliwienie dostępu do danych osobowych podmiotom do tego nieupoważnionym;
    c. zaniechanie, choćby nieumyślne, dopełnienia obowiązku ochrony przetwarzanych danych osobowych;
    d. niedopełnienie obowiązku zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
    e. przetwarzanie danych osobowych niezgodnie z założonym zakresem i celem ich zbierania;
    f. spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nieuprawnione kopiowanie danych osobowych;
    g. naruszenie praw osób, których dane są przetwarzane.
9. Administrator prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych w placówce, której wzór stanowi **załącznik nr 9** do Polityki Bezpieczeństwa.

§10
[Zabezpieczenia fizyczne, techniczne i organizacyjne]

1. Celem zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzania danych osobowych w placówce Administrator wprowadza zabezpieczenia fizyczne, techniczne i organizacyjne, których aktualny wykaz stanowi niejawny **załącznik nr 10** do Polityki Bezpieczeństwa.
2. Administrator wraz z Inspektorem Ochrony Danych Osobowych zobowiązują się do regularnego i stałego przeglądu obowiązujących w placówce zabezpieczeń w celu

stałego ich dopracowywania i dostosowywania do pojawiających się zagrożeń i ryzyka naruszenia danych osobowych.

3. Administrator w celu zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzanych danych osobowych, mając na uwadze, że najważniejsze dla realizacji tego celu jest właściwa praca i postępowanie z danymi osobowymi, będzie prowadzić szkolenia dla osób upoważnionych do przetwarzania danych osobowych z tego zakresu, w tym w szczególności do przeprowadzania szkoleń z tego zakresu i uwrażliwiania pracowników Administratora na tę tematykę, zobowiązany jest Inspektor Ochrony Danych Osobowych.
4. Zgodnie z ust. 3 niniejszego paragrafu Administrator prowadzi rejestr odbytych szkoleń, którego wzór stanowi **załącznik nr 11** do Polityki Bezpieczeństwa.

§11
[Naruszenie przetwarzania danych osobowych]

1. W przypadku stwierdzenia prawdopodobieństwa wystąpienia naruszenia zasad ochrony danych osobowych, osoba która dokonała tego ustalenia zobowiązana jest niezwłocznie powiadomić o swoich przypuszczeniach Administratora, jednakże nie później niż do końca dnia, w którym wystąpiło przypuszczenie wystąpienia naruszenia.
2. Administrator dokonuje oceny zgłoszenia lub własnych ustaleń w zakresie wystąpienia ewentualnego naruszenia i wykazania jego przesłanek, w szczególności oceny ryzyka naruszenia przez nie praw lub wolności osób fizycznych.
3. W każdej sytuacji, w której zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator zgłasza bez zbędnej zwłoki fakt naruszenia zasad ochrony danych osobowych w placówce organowi nadzorczemu, tj. nie później niż w terminie 72 godzin po stwierdzeniu naruszenia (po przeprowadzeniu wewnętrznej analizy, z której uzyskano informację, że doszło do naruszenia).
4. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator zawiadamia o incydencie także osobę, której dane dotyczą.
5. Administrator dokumentuje czynności podjęte w ramach niniejszego paragrafu, a wzór rejestru naruszeń stanowi **załącznik nr 12** do Polityki Bezpieczeństwa
6. Rejestru naruszeń, o którym mowa w §11 ust. 5 Polityki Bezpieczeństwa prowadzi Inspektor Ochrony Danych Osobowych w formie elektronicznej, w szczególności stosując do niego szczegółowe postanowienia wynikające z przyjętej procedury postępowania w przypadku wystąpienia naruszenia.
7. Procedurę postępowania w przypadku wystąpienia naruszenia stanowi **załącznik nr 13** do Polityki Bezpieczeństwa.

§12
[Powierzenie przetwarzania danych]

1. Administrator może powierzyć przetwarzanie danych osobowych innemu podmiotowi, w przypadku zawarcia umowy powierzenia w formie pisemnej.

2. Podmiot taki (zwany Podmiotem Przetwarzającym) może przetwarzać dane tylko i wyłącznie w zakresie i celu przewidzianym w umowie przez Administrator.
3. Administrator przed zawarciem umowy powierzenia zweryfikuje stan zabezpieczeń i poziom ochrony przetwarzania danych osobowych zapewniany przez Podmiot Przetwarzający.
4. Administrator zapewni sobie w umowie możliwość kontroli stanu przetwarzania powierzonych danych osobowych przez Podmiot Przetwarzający.
5. Wzór umowy powierzenia stanowi **załącznik nr 14** do Polityki Bezpieczeństwa.

§13
[Postanowienia końcowe]

1. Polityka Bezpieczeństwa w formie tradycyjnej została sporządzona w jednym egzemplarzu, który przechowywany jest w siedzibie Administratora.
2. Polityka Bezpieczeństwa przechowywana jest także w formie elektronicznej.
3. Politykę Bezpieczeństwa stosuje się niezależnie od tego, czy w związku z przetwarzaniem danych osobowych placówka pełni funkcję administratora, podmiotu przetwarzającego czy odbiorcy danych.
4. Polityka Bezpieczeństwa wchodzi w życie z dniem 25 maja 2018 r.
5. Polityka Bezpieczeństwa obowiązuje do czasu jej zmiany lub uchylenia.

Lista Załączników

Załącznik nr 1 Infografiki - Zasady postępowania i przetwarzania danych

Załącznik nr 2 Wzór obowiązku informacyjnego (klauzuli informacyjnej)

Załącznik nr 3 Instrukcja Zarządzania System Informatycznym

Załącznik nr 4 Wykaz obowiązków Inspektora Ochrony Danych Osobowych

Załącznik nr 5 Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar przetwarzania (załącznik niejawny)

Załącznik nr 6 Wykaz programów komputerowych stosowanych do przetwarzania danych osobowych

Załącznik nr 7 Wzór upoważnienia do przetwarzania danych osobowych

Załącznik nr 8 Wzór oświadczenia osoby upoważnionej do przetwarzania danych osobowych

Załącznik nr 9 Ewidencja osób upoważnionych do przetwarzania danych osobowych

Załącznik nr 10 Wykaz zabezpieczeń fizycznych, organizacyjnych i technicznych (załącznik niejawny)

Załącznik nr 11 Rejestr odbytych szkoleń

Załącznik nr 12 Rejestr naruszeń

Załącznik nr 13 Procedura postępowania z naruszeniami

Załącznik nr 14 Wzór umowy powierzenia