Załącznik nr 1 do zarządzenia
nr 18/2017.2018 Dyrektora Zespołu Szkół
Gołaszynie z dnia 25 maja 2018 r.

Zatwierdzam dokument o nazwie:

Polityka ochrony danych

w

Zespole Szkół

w Gołaszynie

Gołaszyn, 25 maja 2018 r.

Spis treści

I. Podstawy prawne

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE l119 z 4 maja 2016 r., dalej również jako: „**RODO**").
2. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2018.1000 z dnia 2018.05.24).

II. Wstęp

Polityka ochrony danych została wprowadzona w celu wykonania obowiązków nałożonych na Administratora przez powszechnie obowiązujące przepisy prawa, w szczególności 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.

Polityka jest wewnętrznym dokumentem regulującym zasady przetwarzania i ochrony danych osobowych u Administratora.

Polityka została opracowana i wdrożona w celu uzyskania standardu przetwarzania informacji zawierających dane osobowe zgodnego z RODO i odpowiednimi regulacjami krajowymi.

Wdrożenie Polityki stanowi jedną z podstaw wykazania przetwarzania danych osobowych przez Administratora zgodnie z RODO Administrator – przy uwzględnieniu charakteru, zakresu, kontekstu i celu przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia.

Polityka określa w szczególności:

1. Prawa, obowiązki oraz granice dopuszczalnego zachowania osób przetwarzających dane osobowe oraz konsekwencje naruszenia przepisów o ochronie danych osobowych;
2. Sposób przetwarzania danych osobowych oraz zasady postępowania zapewniające ochronę tych danych;
3. Zabezpieczenia i środki ochrony danych osobowych;

4. Zasady rejestrowania czynności przetwarzania danych osobowych;
5. Zasady postępowania w sytuacji naruszenia ochrony danych osobowych.

Zastosowane zabezpieczenia mają zapewnić:

1. Poufność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie są udostępniane nieupoważnionym osobom;
2. Integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
3. Rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
4. Integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji zamierzonej, jak i przypadkowej;
5. Dostępność informacji – rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
6. Zarządzanie ryzykiem – rozumiane jako proces identyfikowania, monitorowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa informacji, które może dotyczyć systemów informatycznych i organizacyjnych służących do przetwarzania danych osobowych.

Administrator będzie przetwarzał dane osobowe z zachowaniem następujących zasad:

1. Zgodności z prawem;
2. Rzetelności;
3. Przejrzystości;
4. Ograniczoności celu;
5. Adekwatności, prawidłowości i okresowości przetwarzanych danych;
6. Poufności, integralności i rozliczalności danych.

Polityka zostanie zaktualizowana w przypadku zmiany przepisów prawa w zakresie ochrony danych osobowych lub w przypadku zmiany okoliczności faktycznych uzasadniających dokonanie takiej zmiany.

Stosowanie Polityki obowiązuje wszystkich pracowników lub współpracowników Administratora mających dostęp do danych osobowych.

Nie jest dopuszczalne naruszanie zasad określonych w Polityce z uwagi na odrębne procedury lub regulacje wewnętrzne Administratora. Żadna procedura ani regulacja wewnętrzna obowiązująca u Administratora nie może naruszać zasad określonych w niniejszej Polityce.

Dane osobowe chronione Polityką przetwarzane są w siedzibie Administratora oraz w miejscach wykonywania pracy przez pracowników Administratora.

III. Obowiązki z zakresu zapewnienia przestrzegania zasad ochrony danych osobowych

I. Administrator:

1. Zapewnia środki niezbędne do stworzenia i funkcjonowania systemu ochrony danych osobowych;
2. Wdraża środki organizacyjne i techniczne niezbędne do zapewnienia rozliczalności, integralności oraz poufność przetwarzanych danych osobowych;
3. Zapewnia wyposażenie systemu informatycznego w środki techniczne zapewniające stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych, których dane są przetwarzane;
4. Wdraża środki organizacyjne, zapewniające stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych;
5. Wymaga od osób, którym polecił przetwarzanie danych osobowych, aby przestrzegały przepisów o ochronie danych osobowych;
6. Dba, aby dostępu do danych osobowych udzielano wyłącznie osobom upoważnionym do ich przetwarzania;
7. Podejmuje działania mające na celu to, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14 RODO, oraz prowadzić z nią wszelką komunikację na mocy art. 15–22 i 34 RODO w sprawie przetwarzania;
8. Zapewnia, by Inspektor Ochrony Danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych;
9. Zapewnia IOD wykonywanie jego zadań w sposób niezależny;
10. Zatwierdza politykę oraz dokumenty opracowywane na jej podstawie.
11. Prowadzi wykaz podmiotów przetwarzających dane;
12. Prowadzi rejestr czynności przetwarzania danych osobowych;
13. Prowadzi rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu podmiotu powierzającego.

II. Inspektor Ochrony Danych:

1. Przekazuje Administratorowi oraz jego pracownikom informacje o spoczywających na nich obowiązkach z zakresu ochrony danych osobowych
2. Monitoruje przestrzegania przez Administratora i jego pracowników przepisów o ochronie danych osobowych - poprzez wykonywanie cyklicznych audytów i sprawdzeń;

3. Informuje Administratora o wynikach przeprowadzanych audytów i sprawdzeń;
4. Wspiera Administratora przy wdrażaniu zabezpieczeń będących wynikiem cyklicznych audytów oraz analizy ryzyka;
5. Prowadzi działania zwiększające świadomość pracowników Administratora z zakresu ochrony danych osobowych oraz informuje ich o zagrożeniach związanych z przetwarzaniem danych osobowych;
6. Udziela zaleceń co do oceny skutków dla ochrony danych oraz monitoruje jej wykonania, zgodnie z art. 35 RODO;
7. Współpracuje z organem nadzorczym;
8. Pełni rolę punktu kontaktowego dla organu nadzorczego w sprawach z zakresu przetwarzania danych osobowych;
9. Pełni rolę punktu kontaktowego dla osób, których dane dotyczą;
10. Reaguje na zgłaszane incydenty związane z naruszeniem ochrony danych osobowych w sposób adekwatny do zaistniałego incydentu (po przeanalizowaniu jego przyczyny i możliwych skutków);
11. Aktualizuje politykę;
12. Sporządza i aktualizuje informacje podawane w związku ze zbieraniem danych osobowych od osoby, której dane dotyczą;
13. Sporządza i aktualizuje informacje podawane w związku ze zbieraniem danych od osobowych w sposób inny niż od osoby, której dane dotyczą.

III. Osoba odpowiedzialna za nadzorowanie systemu informatycznego:

1. Nadzoruje, aby w systemie informatycznym wykorzystywane były środki techniczne i organizacyjne zapewniające ochronę danych osobowych przetwarzanych w systemie informatycznym;
2. Zapewnia bieżące utrzymanie systemów informatycznych wykorzystywanych do przetwarzania danych osobowych;
3. Dba, aby dane przesyłane za pośrednictwem urządzeń teletransmisji oraz sieci komputerowej przesyłane były w sposób zapewniający bezpieczeństwo wymiany danych;
4. Nadzoruje funkcjonowanie mechanizmów uwierzytelniania użytkowników w systemie informatycznym;
5. Wykonuje kopie bezpieczeństwa elektronicznych zbiorów danych osobowych;
6. Przechowuje kopie bezpieczeństwa i logów danych;
7. Przydziela pracownikom Administratora identyfikatory i hasła do systemu informatycznego, modyfikuje uprawnienia do systemu informatycznego, usuwa konta użytkowników;
8. Prowadzi ewidencję użytkowników systemów informatycznych wykorzystywanych do przetwarzania danych osobowych;

9. Dba o prawidłowe (zgodne z wymogami przepisów o ochronie danych osobowych) naprawy, konserwacje oraz likwidację urządzeń elektronicznych, dysków lub innych nośników informacji zawierających dane osobowe;
10. Dba o wykorzystywanie przez Administratora i jego pracowników legalnego oprogramowania;
11. Zarządza licencjami do systemu informatycznego;
12. Zapewnia właściwą konfigurację systemów zarządzania hasłami;
13. Inwentaryzuje sprzęt komputerowy oraz systemy informatyczne;
14. W przypadku wystąpienia incydentu z zakresu ochrony danych osobowych – wspólnie z IOD prowadzi postępowanie wyjaśniające w powyższym zakresie.

IV. Osoba upoważniona do przetwarzania danych osobowych:

1. Przestrzega przyjęte u Administratora zasady ochrony danych osobowych;
2. Przestrzega zasad bezpieczeństwa przetwarzania danych osobowych;
3. Informuje bezpośredniego przełożonego lub IOD o incydentach z zakresu bezpieczeństwa danych osobowych;
4. Dba o przetwarzanie danych osobowych ze szczególną starannością - w celu ochrony interesów osób, których dane są przetwarzane;
5. Zachowa w poufności przetwarzane dane osobowe oraz informacje o sposobie ich zabezpieczania;
6. Usuwa dane osobowe, jeżeli Administrator nie posiada interesu prawnego i faktycznego w przetwarzaniu (w tym archiwizacji) tych danych – w przypadku wątpliwości co do zasadności usunięcia danych osobowych osoba upoważniona zwraca się o opinię do IOD;
7. Przestrzega Polityki „czystego biurka”;
8. Po zakończeniu pracy porządkuje swoje stanowisko pracy i zabezpiecza przetwarzane dane osobowe – w sposób adekwatny do zastosowanych rozwiązań technicznych i organizacyjnych, (tj. m.in.: wyłącza i zabezpiecza komputer, zabezpiecza nośniki danych, zamyka na klucz szafy, w których przechowywane są dane osobowe, umieszcza klucz do ww. szaf w miejscu wskazanym przez Administratora, zamyka okna i drzwi).

V. Ogólne zasady przetwarzania danych osobowych

1. Dane osobowe mogą być wykorzystywane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane.
2. Zakres przetwarzania danych osobowych jest ograniczony do danych, które są niezbędne do osiągnięcia celu przetwarzania danych. Zabronione jest pozyskiwanie zbyt szczegółowych danych osobowych, tj. takich, które nie są niezbędne dla celu, w którym zostały zebrane (zasada minimalizacji danych osobowych).
3. Każdy pracownik Administratora, który zauważy, że ma dostęp do danych osobowych, które

nie są mu potrzebne w pracy ma obowiązek poinformować o tym fakcie Administratora.

4. Po wykorzystaniu, dane osobowe powinny być przechowywane w formie uniemożliwiającej identyfikację osób, których dotyczą, zniszczone lub, w przypadku powierzenia, zwrócone podmiotowi, który dane powierzył.
5. Zasady ochrony danych osobowych określone przez politykę mają zastosowanie do:
    a) Wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów;
    b) Przetwarzania informacji zawierających dane osobowe, w tym systemów IT;
    c) Informacji będących własnością Administratora oraz przetwarzanych przez niego w związku z prowadzoną działalnością;
    d) Wszystkich lokalizacji, budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;
    e) Wszystkich osób świadczących pracę lub wykonujących czynności na rzecz Administratora mających dostęp do informacji podlegających ochronie.
6. Wszystkie osoby, które posiadają dostęp do danych osobowych muszą posiadać upoważnienie do przetwarzania danych nadane przez Administratora oraz podpisać oświadczenie o zachowaniu poufności. Wzór upoważnienia oraz wzór oświadczenia zawarte zostały w załączniku do Polityki.

VI. Podstawy dopuszczalności przetwarzania danych osobowych

Administrator przetwarza dane osobowe jedynie jeżeli przetwarzanie jest uprawnione na podstawie co najmniej jednej z przesłanek określonych w art. 6 ust. 1 RODO. W szczególności podstawę przetwarzania danych osobowych stanowi: a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów; b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy; c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze.

Zgoda na zbieranie danych osobowych

1. Zgoda na przetwarzanie danych osobowych nie może być domniemana lub dorozumiana ani wynikać z oświadczenia woli o innej treści.
2. Zgoda na przetwarzanie danych osobowych powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, należy pozyskać odrębną zgodę na każdy cel.
3. Zgoda na przetwarzanie danych osobowych może być odwołana w każdym czasie w sposób tak samo prosty i przystępny, w jaki została pozyskana.

Zbieranie danych w celu wykonania umowy

1. Administrator ma prawa do przetwarzania danych osobowych, jeżeli jest to niezbędne do wykonania umowy, gdy osoba, której dane dotyczą, jest jej stroną, jak również działania takie

są legalne, gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą.

2. W przypadku przetwarzania danych osobowych niezbędnego do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą, dopuszczalność przetwarzania danych osobowych została uzależniona od spełnienia następujących przesłanek:
    a) przetwarzanie jest niezbędne do podjęcia działań przed zawarciem umowy,
    b) zawarcie umowy następuje na żądanie osoby, której dane dotyczą.

Obowiązek prawny ciążący na Administratorze

1. Administrator ma prawo do przetwarzania danych osobowych, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. W przypadku, gdy Administrator danych osobowych przetwarza dane dla spełnienia obowiązku wynikającego z przepisów prawa, określenie celu przetwarzania danych osobowych powinno nastąpić przez odwołanie się do okoliczności konkretnej sprawy, z którą związane jest przetwarzanie danych. Jeżeli przetwarzanie danych jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze, nie powinno się występować o zgodę osoby, której dane dotyczą, na przetwarzanie jej danych osobowych. Może to bowiem prowadzić m.in. do mylnego przekonania o swobodzie w zakresie podania danych, w sytuacji gdy obowiązek ich podania wynika z powszechnie obowiązujących przepisów prawa.
2. Przetwarzanie danych osobowych na podstawie przepisów prawa jest dopuszczalne pod warunkiem łącznego spełnienia następujących przesłanek:
    a) istnieje przepis prawa, który nakłada na Administratora danych obowiązek prawny,
    b) przetwarzanie danych jest niezbędne dla realizacji tego obowiązku prawnego.

VII. Obowiązek informacyjny

W przypadku zbierania danych osobowych od osoby, której one dotyczą, pracownik Administratora, który pozyskuje dane jest obowiązany poinformować tę osobę o tożsamości Administratora i o jego danych kontaktowych, o celach i podstawie przetwarzania danych, a jeżeli przetwarzanie odbywa się na tej podstawie, że jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora danych osobowych lub przez stronę trzecią – o tych prawnie uzasadnionych interesach, o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją, o okresie czasu, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu, o prawie do żądania od Administratora danych osobowych dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych, o prawie do cofnięcia zgody w dowolnym momencie (jeżeli przetwarzanie odbywa się na podstawie zgody), o prawie wniesienia skargi do organu nadzorczego, o

tym, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych.

Realizacja obowiązku informacyjnego

Obowiązek informacyjny realizowany jest, w zależności od formy kontaktu Administratora z osobą, której dane dotyczą poprzez:

1. Umieszczenie wymaganych informacji na stronie internetowej Administratora;
2. Głosowe przekazanie wymaganych informacji osobie telefonicznie kontaktującej się z Administratorem;
3. Umieszczenie wymaganych informacji w sali obsługi klientów Administratora – w widocznym i łatwo dostępnym miejscu;
4. W przypadku komunikacji za pośrednictwem poczty e-mail – przez 1) przekazanie wymaganych informacji jako załącznik do pierwszej wiadomości przekazywanej osobie fizycznej za pośrednictwem poczty elektronicznej w danej sprawie, informacja o zawartości załącznika winna zostać wskazana w treści wiadomości e-mail bądź 2) poprzez ustawienie funkcji autorespondera – każdorazowe odesłanie obowiązku informacyjnego po przesłaniu na skrzynkę mailową Administratora wiadomości e-mail lub 3) umieszczenie wymaganych informacji w stopce wiadomości e-mail;
5. Wysłanie wymaganych wiadomości w wersji papierowej – wraz z pierwszym pismem kierowanym do osoby fizycznej w prowadzonej przez Administratora sprawie lub/oraz wraz z dokumentem kończącym postępowanie w sprawie prowadzonej z wniosku lub przy udziale osoby fizycznej w danej instancji.

Wzór informacji przekazywanej osobie fizycznej stanowi załącznik do Polityki.

VIII. Powierzenie przetwarzania danych podmiotom trzecim

Powierzenie przetwarzania danych osobowych podmiotowi trzeciemu może nastąpić tylko na podstawie prawnej, która zostanie zweryfikowana przed dokonaniem czynności powierzenia. Wzór umowy powierzenia stanowi załącznik do Polityki. Umowa może zostać podpisana po upewnieniu się, że dane osobowe mogą zostać legalnie przekazane.

Powierzania danych rejestrowane są w wykazie podmiotów, którym powierzono dane osobowe, za każdym razem, gdy takie powierzenie nastąpi.

Wzór wykazu podmiotów, którym powierzono dane osobowe stanowi załącznik do Polityki.

Obowiązek rejestrowania czynności przetwarzania danych

Zgodnie z wymogami RODO Administrator prowadzi rejestr czynności przetwarzania danych - dla danych, w stosunku do których występuje jako Administrator danych osobowych, jak i dla danych, w stosunku do których jest podmiotem przetwarzającym dane osobowe.

Kierownik wydziału, w którym wykonywane są czynności przetwarzania danych osobowych nieujawnione w prowadzonym przez Administratora rejestrze czynności przetwarzania jest zobowiązany bezzwłocznie zgłosić ten fakt IOD w celu uzupełnienia rejestru czynności przetwarzania.

Wzór rejestru czynności przetwarzania stanowi załącznik do Polityki.

IV. Odpowiedzialność za naruszenie przepisów o ochronie danych osobowych

Za naruszenie ochrony danych osobowych:

1. Administrator może ponieść odpowiedzialność cywilną zgodnie z art. 82 RODO lub odpowiedzialność Administracyjną na podstawie wskazanej w art. 83 lub 84 RODO.
2. Podmiot przetwarzający może ponieść odpowiedzialność cywilną zgodnie z art. 82 RODO lub odpowiedzialność Administracyjną na podstawie wskazanej w art. 83 i 84 RODO.
3. Osoba upoważniona może ponieść odpowiednio odpowiedzialność wskazaną w art. 52 lub 208 kodeksu pracy, odpowiedzialność kontraktową przewidzianą w art. 471 kodeksu cywilnego, albo odpowiedzialność karną przewidzianą w art. 266 kodeksu karnego.

Naruszenie Polityki może zostać potraktowane jako ciężkie naruszenie obowiązków pracowniczych. W szczególności jako ciężkie naruszenie obowiązków pracowniczych może zostać uznane niepowiadomienie odpowiedniej osoby zgodnie z określonymi w polityce zasadami o: 1) wykryciu incydentu lub 2) wykryciu uzasadnionego podejrzenia powstania incydentu lub 3) niepodjęcie określonych w polityce działań, wymaganych w przypadku uzasadnionego podejrzenia powstania incydentu. W powyższych przypadkach może zostać wszczęte postępowanie dyscyplinarne.

Poniesienie odpowiedzialności dyscyplinarnej nie wyklucza poniesienia także odpowiedzialności Administracyjnej, cywilnej lub karnej.

V. Realizacja zasad: 1) poufności, 2) integralności oraz 3) rozliczalności przetwarzania danych osobowych

Administrator dba o zapewnienie 1) poufności, 2) integralności oraz 3) rozliczalności przetwarzanych danych osobowych i zastosowanie w tym celu niezbędnych środków organizacyjnych oraz technicznych.

Zastosowanie odpowiednich środków organizacyjnych i technicznych ma na celu obniżenie poziomu ryzyka wystąpienia incydentów, związanych z bezpieczeństwem przetwarzania danych osobowych. Obniżenie poziomu ryzyka następuje do poziomu akceptowalnego przez Administratora, poprzez wykorzystanie środków adekwatnych z uwagi na występujący stopień ryzyka, stopień bezpieczeństwa przetwarzania danych osobowych oraz koszt wdrożenia środków obniżających ww. stopień ryzyka.

Obniżenie ryzyka naruszenia ochrony danych osobowych następuje w szczególności poprzez:

1. Monitorowanie przez IOD przestrzegania Polityki przez Administratora i pracowników Administratora;
2. Monitorowanie bezpieczeństwa środowiska informatycznego;
3. Upoważnienie pracowników Administratora do przetwarzania danych osobowych zgodnie z zakresem przetwarzania danych osobowych przez nich wykonywanym;
4. Prowadzenie ewidencji upoważnień do przetwarzania danych osobowych;
5. Pobieranie od osób przetwarzających dane osobowe oświadczeń o zachowaniu w poufności danych osobowych i sposobów zabezpieczenia danych, które są zbierane od osób upoważnionych;
6. Szkolenie osób upoważnionych do przetwarzania danych osobowych z zasad bezpiecznego przetwarzania danych osobowych;
7. Zawieranie z podmiotami przetwarzającymi dane w imieniu Administratora umów powierzenia danych osobowych, o których mowa w art. 28 ust. 3 RODO;
8. Prowadzenie ewidencji umów powierzenia;
9. Prowadzenie rejestru czynności przetwarzania danych osobowych, zgodnie z art. 30 RODO;
10. Przestrzeganie zasady, zgodnie z którą w obszarze przetwarzania danych osobowych osoby trzecie przebywają wyłącznie w obecności osoby upoważnionej lub po uprzednim uzyskaniu zgody przez Administratora.

W celu zapewnienia poufności przetwarzania danych osobowych:

1. Administrator korzysta z usług ochrony osób i mienia – w wymiarze i zakresie adekwatnym do potrzeb ochrony obszaru przetwarzania danych;
2. Administrator w celu zapewnienia porządku publicznego i bezpieczeństwa obywateli oraz ochrony przeciwpożarowej i przeciwpowodziowej może stosować środki techniczne umożliwiające rejestrację obrazu (monitoring) w obszarze przestrzeni publicznej, jeżeli jest to konieczne do zapewnienia porządku publicznego i bezpieczeństwa obywateli lub ochrony przeciwpożarowej i przeciwpowodziowej. Nagrania obrazu zawierające dane osobowe przetwarza się wyłącznie do celów dla których zostały zebrane i przechowuje przez okres nieprzekraczający 3 miesięcy od dnia nagrania, o ile przepisy odrębne nie stanowią inaczej;

3. Osoby nieupoważnione nie mają swobodnego dostępu do obszaru przetwarzania danych;
4. Wejście do obszaru przetwarzania danych zabezpieczone jest zamkami patentowymi;
5. Dane osobowe przechowywane w formie papierowej trzymane są w zamykanych szafkach, szafach lub szufladach;
6. Jeden egzemplarz kluczy do szafek, szaf i szuflad, w których trzymane są dane osobowe w formie papierowej przechowywane są w zabezpieczonym, przeznaczonym do tego celu miejscu, drugi egzemplarz ww. kluczy pozostawiony jest w zabezpieczonym depozycie, przez osobę wskazaną przez Administratora;
7. Uzyskanie dostępu do danych w systemie informatycznym wymaga uwierzytelnienia użytkownika;
8. Użytkownicy systemu informatycznego używają haseł składających się z 8 znaków (małe, duże litery, przynajmniej jedna cyfra lub znak specjalny); zmiana hasła wymuszana jest przez system informatyczny, co 30 dni;
9. Na stacjach roboczych, za pomocą których są przetwarzane dane osobowe, zainstalowano oprogramowanie antywirusowe, które automatycznie aktualizuje sygnatury wirusów;
10. System informatyczny jest monitorowany;
11. Dostęp do danych osobowych z sieci publicznej ograniczony jest przez zapory ogniowe (firewall);
12. Zapory ogniowe (firewall) chronią systemy informatyczne przed nieuprawnionym dostępem i atakami z zewnątrz.

W celu zapewnienia integralności przetwarzania danych osobowych:

1. Dane osobowe chronione są przed nieautoryzowanym dostępem;
2. Na stacjach roboczych, za pomocą których pracownicy Administratora przetwarzają dane osobowe działa oprogramowanie antywirusowe automatycznie aktualizujące sygnatury wirusów;
3. Wykorzystywane jest awaryjne podtrzymywanie zasilania serwerów oraz stacji roboczych przy użyciu UPS;
4. Cyklicznie sprawdzana jest możliwość odtworzenia danych z wykonywanych kopii zapasowych.

W celu zapewnienia rozliczalności przetwarzanych danych osobowych:

1. Do danych w systemie informatycznym dostęp mają jedynie uwierzytelnieni użytkownicy;
2. Serwery i stacje robocze posiadają awaryjne zasilanie (UPS);
3. Wykonywany jest zapis zdarzeń w systemach informatycznych.

VI. Przetwarzanie danych osobowych poza obszarem przetwarzania

Przetwarzanie danych osobowych poza obszarem przetwarzania wymaga:

1. Zachowania szczególnej ostrożności podczas transportu, przechowywania i użytkowania nośników zawierających dane osobowe;
2. Zapisywania danych na przenośnych nośnikach danych z zastosowaniem środków ochrony kryptograficznej (szyfrowania) przetwarzanych danych;
3. Szczególnej ochrony nośników danych – niedozwolone jest pozastawianie nośników danych w miejscach powszechnie dostępnych;
4. Wykorzystywania nośników danych wyłącznie w celach służbowych.

W celu zabezpieczania prawidłowości przetwarzania danych osobowych poza obszarem przetwarzania Administrator prowadzi rejestr posiadanych zewnętrznych nośników danych – zgodnie z załącznikiem do Polityki.

VII. Realizacja praw i wolności osób, których dane dotyczą

Administrator dba o to, aby osoba, której dane dotyczą, była informowana o prowadzeniu operacji przetwarzania jej danych osobowych i o celach tego przetwarzania – zgodnie z zasadą rzetelnego i przejrzystego przetwarzania danych osobowych.
Administrator dba, aby osobom których dane dotyczą przekazywano wszelkie informacje, o których mowa w art. 13 i 14 RODO oraz, aby informacje te były przekazywane w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem oraz prowadzi z tymi osobami wszelką komunikację na mocy art. 15–22 i 34 RODO w sprawie przetwarzania.

Administrator dba o realizację praw i wolności osób, których dane dotyczą udzielając tym osobom informacji zgodnie z poniższymi zasadami:

1. Informacje udzielane są na piśmie lub w inny sposób, w tym elektronicznie.
2. Na żądanie osoby, której dane dotyczą informacji można udzielić ustnie, po uprzednim zweryfikowaniu tożsamość osoby, której dane dotyczą.
3. Informacje udzielane są bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania – osobę, której dane dotyczą informuje się o działaniach podjętych w związku z żądaniem na podstawie art. 15–22 RODO.
4. Jeżeli osoba wskazana do udzielenia informacji ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, o którym mowa w art. 15–21, powinna zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.

5. W przypadku przetwarzania niewymagającego identyfikacji, tam gdzie Administrator nie jest w stanie zidentyfikować podmiotu danych, można odmówić podjęcia żądanego działania.
6. Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, przedstawia się tej osobie klauzule informacyjne o treści i w miejscach lub dokumentach wskazanych w załączniku do Polityki.
7. W przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą, przedstawia się jej klauzule informacyjne o treści i w miejscach lub dokumentach wskazanych w załączniku do Polityki.
8. Jeżeli Administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane zostały pozyskane, przed dalszym przetwarzaniem informuje osobę której dane dotyczą o tym innym celu oraz udziela jej wszelkich innych stosowanych informacji. Administrator, bez zbędnej zwłoki, informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

Na wniosek osoby, której dane dotyczą Administrator informuje tę osobę czy Administrator przetwarza dane osobowe dotyczące tej osoby.

Osoba fizyczna jest uprawniona do uzyskania dostępu do jej danych osobowych oraz uzyskania informacji, określających:

1. Cele przetwarzania;
2. Kategorie przetwarzanych danych osobowych;
3. Odbiorców lub kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności odbiorców w państwach trzecich lub o organizacjach międzynarodowych;
4. W miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
5. Prawo do żądania od Administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
6. Prawo wniesienia skargi do organu nadzorczego;
7. Jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
8. Informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Osoba, której dane dotyczą, ma prawo:

1. Żądania od Administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądać, aby jej niekompletne dane osobowe zostały uzupełnione - w tym poprzez przedstawienie dodatkowego oświadczenia (prawo do sprostowania danych);
2. Żądania od Administratora niezwłocznego usunięcia dotyczących jej danych osobowych. Administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe (prawo do usunięcia danych), jeżeli zachodzi jedna z następujących okoliczności:
    a) Dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
    b) Osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie, i nie ma innej podstawy prawnej przetwarzania jej danych osobowych;
    c) Osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 RODO wobec przetwarzania;
    d) Dane osobowe były przetwarzane niezgodnie z prawem;
    e) Dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego, któremu podlega Administrator;
    f) Dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.

W przypadku upublicznienia danych osobowych przez Administratora, które ma on obowiązek usunąć, Administrator – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających, że osoba, której dane dotyczą, żąda, by usunięte wszelkie łącza do jej danych, kopie tych danych osobowych lub ich replikacje.

Wyjątek:

Prawo do usunięcia danych nie ma zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:

- Do korzystania z prawa do wolności wypowiedzi i informacji;
- Do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa, któremu podlega Administrator, lub do wykonania zadania realizowanego w interesie publicznym;
- Do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, o ile prawdopodobne jest, że realizacja

prawa do bycia zapomnianym uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub

- Do ustalenia, dochodzenia lub obrony roszczeń.

3. Osoba, której dane dotyczą, ma prawo żądania od Administratora ograniczenia przetwarzania jej danych osobowych w następujących przypadkach („prawo do ograniczenia przetwarzania”):
    a) Osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – przez okres pozwalający Administratorowi na sprawdzenie prawidłowości danych;
    b) Przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
    c) Administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
    d) Osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie Administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

    Jeżeli zgodnie z żądaniem przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.

    Przed uchyleniem ograniczenia przetwarzania Administrator informuje o tym osobę, której dane dotyczą, która żądała ograniczenia przetwarzania.

4. Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła Administratorowi, oraz ma prawo przesłać te dane osobowe innemu Administratorowi bez przeszkód ze strony Administratora, któremu dostarczono te dane osobowe („prawo do przenoszenia danych”), jeżeli:
    a) Przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy; oraz
    b) Przetwarzanie odbywa się w sposób zautomatyzowany.

    Wykonując prawo do przenoszenia danych osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez Administratora bezpośrednio innemu Administratorowi, o ile jest to technicznie możliwe.

Wykonanie prawa do przenoszenia danych, pozostaje bez uszczerbku prawa do bycia zapomnianym. Prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi.

Administrator odmawia realizacji prawa do przenoszenia danych w sytuacji, gdy realizacja tego prawa może niekorzystnie wpływać na prawa i wolności innych osób.

5. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych („prawo do sprzeciwu"), gdy:
    a) Przetwarzanie danych jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi;
    b) Przetwarzanie danych jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

    Wyjątek:
    Administratorowi nie wolno przetwarzać danych osobowych w sytuacji skorzystania z prawa do sprzeciwu, chyba że wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

    Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych osoba, której dane dotyczą, ma prawo wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

    Procedura weryfikacji tożsamości osoby, która złożyła wniosek stanowi załącznik do Polityki.

VIII. Przetwarzanie danych osobowych przy użyciu narzędzi pracy

1. Pracownik Administratora przetwarza dane osobowe wykorzystując sprzęt (w tym komputerowy) oraz oprogramowanie udostępnione mu przez Administratora (dalej jako

„narzędzia pracy”). Pracownik ma dostęp do informacji stanowiących: tajemnicę, dane osobowe, dane poufne lub dane, co do których Administrator zobowiązał się do ich zabezpieczenia przed nieuprawnionym ujawnieniem w zakresie niezbędnym do wykonywania przez pracownika jego obowiązków pracowniczych.

2. Pracownik może korzystać z narzędzi pracy wyłącznie w celu wykonywania powierzonych obowiązków, zgodnie z obowiązującymi przepisami prawa.
3. Pracownik nie jest uprawniony do:
    a) Korzystania z oprogramowania komputerowego innego niż udostępnione przez Administratora;
    b) Korzystania z narzędzi pracy w celach prywatnych;
    c) Prowadzenie prywatnej korespondencji e-mail przy użyciu narzędzi pracy, korzystania z komunikatorów, portali społecznościowych lub stron internetowych innych niż wymagane do wykonywania obowiązków pracowniczych;
    d) Korzystania z narzędzi pracy w sposób mogący naruszyć prawa osób trzecich;
    e) Kopiowania i udostępniania osobom trzecim udostępnionego przez Administratora oprogramowania komputerowego.
4. Administrator jest uprawniony do kontroli prawidłowego wykorzystywania przez jego pracownika narzędzi pracy poprzez:
    a) Monitoring operacji wykonywanych przy użyciu narzędzi pracy;
    b) Kontrolę korzystania z narzędzi pracy;
    c) Kontrolę czasu pracy wykonywanej przy użyciu narzędzi pracy;
    d) Monitorowanie korzystania z sieci Internet;
    e) Kontrolę prowadzonej przy użyciu narzędzi pracy korespondencji e-mail.
5. Kategorycznie zabronione jest wykorzystywanie narzędzi pracy w celach niezgodnych z prawem lub zasadami obowiązującymi u Administratora, a w szczególności poprzez korzystanie ze służbowej poczty w celach prywatnych oraz w sposób naruszający prawa autorskie (nielegalne pobieranie bądź udostępniania plików) lub powodujący zainfekowanie sieci komputerowej wirusami komputerowymi.
6. Naruszenie przez pracownika jego obowiązków pracowniczych w zakresie wskazanym w polityce może stanowić podstawę do podjęcia przez Administratora przysługujących mu środków prawnych, a w szczególności może stanowić przyczynę uzasadniającą wypowiedzenie przez Administratora umowy o pracę łączącej go z pracownikiem lub wymierzenie kary porządkowej przewidzianej przepisami ustawy z dnia 26 czerwca 1974 r. Kodeks pracy.

IX. Warunki korzystania z systemu informatycznego

1. Zasady zachowania bezpieczeństwa w systemie informatycznym obejmują wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę informacji przed ich nieuprawnionym przetwarzaniem.
2. Zgodnie z postanowieniami Polityki, zabrania się użytkownikowi systemu informatycznego podejmowania jakichkolwiek czynności mających na celu naruszenie bezpieczeństwa przetwarzanych danych, w tym prób przełamania zabezpieczeń tego systemu.
3. W celu zapobieżenia nieautoryzowanemu dostępowi do systemu informatycznego pracownik nie może przechowywać danych służących do logowania do systemu w miejscach dostępnych dla innych osób oraz ujawniać danych służących do logowania innym osobom.
4. Zabronione jest korzystanie z systemu informatycznego z użyciem danych dostępowych innego pracownika.
5. Pracownicy są zobowiązani do ustawienia ekranów monitorów w taki sposób, aby uniemożliwić osobom postronnym wgląd lub spisanie informacji aktualnie wyświetlanej na ekranie monitora.
6. Pracownik zobowiązany jest do przestrzegania zasady „czystego biurka”, w szczególności przed opuszczeniem swego stanowiska pracy powinien schować wszelkie dokumenty oraz informatyczne nośniki danych do zamykanej szafy.
7. W czasie kopiowania, drukowania dokumentów zawierających dane osobowe, pracownik zobowiązany jest do zachowania zasady „czystej drukarki”, „czystej kopiarki”, w szczególności przed opuszczeniem stanowiska kopiowania/drukowania upewnić się, że w urządzeniach nie pozostały dokumenty zawierające dane osobowe.
8. Przed przystąpieniem do realizacji zadań związanych z przetwarzaniem danych osobowych z użyciem urządzeń mobilnych, pracownik jest zobowiązany do sprawdzenia, czy posiadane przez niego dane są należycie zabezpieczone przed dostępem osób nieupoważnionych.
9. Po zakończeniu przetwarzania danych osobowych, pracownik zobowiązany jest do należytego zabezpieczenia ich przed dostępem osób nieupoważnionych.
10. Przetwarzanie danych osobowych za pomocą urządzeń przenośnych może odbywać się poza obszarem siedziby Administratora wyłącznie za jego zgodą. Pracownik użytkujący urządzenia przenośne zawierające dane osobowe zachowuje szczególną ostrożność podczas transportu, przechowywania i użytkowania poza siedzibą firmy i ma całkowity zakaz pozostawiania tych urządzeń bez nadzoru.
11. Każde urządzenie przenośne musi być zabezpieczenie co najmniej hasłem.
12. Bezwzględnie zabrania się łamania lub obchodzenia zabezpieczeń systemów informatycznych. O każdym przypadku znalezienia luki w zabezpieczeniach pracownik ma obowiązek powiadomić IOD.
13. Sprzęt elektroniczny zawierający dane osobowe (urządzenia, dyski oraz inne elektroniczne

nośniki informacji) przeznaczone do:

a) Likwidacji – pozbawia się wcześniej zapisu danych osobowych, a gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający odczytanie danych;
b) Przekazania podmiotowi, który nie jest uprawniony do przetwarzania danych – pozbawia się wcześniej zapisu danych w sposób uniemożliwiający ich odzyskanie;
c) Naprawy – pozbawia się wcześniej zapisu danych osobowych w sposób umożliwiający odzyskanie danych.

X. Nadawania i odbierania uprawnień

1. Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych nadaje osoba wskazana przez Administratora.
2. Upoważnienie do przetwarzania danych udzielane jest jedynie w zakresie niezbędnym do wykonywania przez pracownika jego obowiązków służbowych, wzór upoważnienia stanowi załącznik do Polityki.
3. Administrator prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, wzór ewidencji stanowi załącznik do Polityki. W ewidencji odnotowuje się niezwłocznie zarówno fakt nadania upoważnienia, jak i cofnięcia upoważnienia.
4. Upoważnienie do przetwarzania danych osobowych przechowuje się wraz z dokumentacją Administratora z zakresu ochrony danych osobowych.
5. Nadanie uprawnień do systemu informatycznego polega na przydzieleniu unikalnego identyfikatora i hasła.
6. Administrator prowadzi ewidencję osób uprawnionych do przetwarzania danych osobowych w systemie informatycznym. Ewidencja zawiera w szczególności: identyfikator użytkownika systemu, datę i godzinę nadania oraz odebrania uprawnień. Wzór ewidencji stanowi załącznik do Polityki.
7. Odebranie uprawnień następuje przez:
    a) Zablokowanie konta pracownika do czasu ustania przyczyny uzasadniającej blokadę (odebranie uprawnień czasowe),
    b) Usunięcie danych pracownika z bazy użytkowników systemu (odebranie uprawnień trwałe).
8. Identyfikator pracownika, któremu odebrano uprawnienia trwale, należy niezwłocznie usunąć oraz unieważnić jego hasło.

XI. Procedura dostępu do danych osobowych w systemie informatycznym

1. Rozpoczęcie pracy pracownika w systemie informatycznym obejmuje uruchomienie komputera, wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu. Pracownikowi nie wolno w czasie uruchamiania systemu operacyjnego odchodzić od stanowiska. Jest to dozwolone tylko i wyłącznie zgodnie z procedurą opisującą tryb zawieszenia pracy z systemem, w którym przetwarzane są dane osobowe.
2. W identyfikatorze nie są używane znaki diakrytyczne (tzn. polskie znaki).
3. W przypadku trzech nieudanych prób uwierzytelnienia hasła, celem zabezpieczenia systemu przed próbą włamania, następuje automatyczne zablokowanie dostępu pracownika do systemu. Odblokowanie dostępu pracownika do systemu wymaga interwencji uprawnionego pracownika pracodawcy.
4. W systemie stosuje się uwierzytelnianie co najmniej jednostopniowe: na poziomie dostępu do sieci lokalnej.
5. W zakresie jakim jest to możliwe stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do sieci lokalnej oraz dostępu do aplikacji lub programu.
6. W zakresie jakim jest to możliwe identyfikator pracownika w aplikacji i programie (o ile działanie aplikacji lub programu na to pozwala) powinny być tożsame z identyfikatorem przydzielonym w sieci lokalnej.
7. Hasło pracownika powinno być zmieniane nie rzadziej niż co 30 dni.
8. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł. Zabronione jest udostępnianie przez pracownika identyfikatora lub hasła innym osobom, a także korzystanie z identyfikatora i hasła innego pracownika. Zabrania się przechowywania haseł w miejscach dostępnych innym osobom, np. pod klawiaturą, na monitorze lub w niezabezpieczonej szafce.
9. Jeżeli pracownik podejrzewa, że jego hasło zostało poznane przez osobę trzecią w sposób nieuprawniony, to jest on zobowiązany do samodzielnej zmiany hasła i powiadomienia o tym incydencie Administratora.
10. Hasło powinno składać się z zestawu co najmniej ośmiu znaków, zawierać małe i duże litery oraz cyfry i znaki specjalne. Hasło nie może być identyczne z identyfikatorem pracownika w jakiejkolwiek formie (pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę itp.), ani jego imieniem lub nazwiskiem.
11. Niedozwolone jest stosowanie haseł, którymi pracownik posługiwał się uprzednio w okresie minionego roku.
12. Kombinacja hasła nie powinna zwierać ogólnie dostępnych informacji o pracowniku, np. Imienia i nazwiska, numeru telefonu, numeru rejestracyjnego samochodu, marki samochodu lub przewidywanych sekwencji z klawiatury (np.: „qwerty”„12345”, „1111” itp.).
13. Nie należy korzystać z opcji zapamiętywania hasła w systemie.
14. Dostęp do systemu informatycznego jest odbierany pracownikowi nie później niż w dniu ustania jego zatrudnienia u Administratora. Po ustaniu stosunku pracy hasło Administratora systemu zostaje zmienione przez osobę uprawnioną.

15. Rozpoczęcie pracy w systemie informatycznym odbywa się po prawidłowym uwierzytelnieniu pracownika w systemie informatycznym.
16. Każdorazowe zaprzestanie pracy w systemie informatycznym, wymaga zabezpieczenia systemu przed nieuprawnionym dostępem, np. poprzez zablokowanie stacji roboczej przy użyciu komendy „ctrl+alt+del i zablokuj komputer". Pracownik jest zobowiązany wyłączyć monitor w sytuacji, gdy wgląd w wyświetlane na monitorze dane może mieć osoba nieuprawniona. Na komputerze pracownika niewykonującego żadnych czynności przez 10 minut zostanie automatycznie uruchomiony wygaszacz ekranu.
17. Zakończenie pracy polega na wybraniu odpowiedniego polecenia systemowego umożliwiającego zakończenie pracy. Zaleca się zamknięcie wszystkich programów i zapisanie wszystkich otwartych plików. Pracownik powinien zaczekać przy komputerze do chwili jego wyłączenia.
18. Pracownik udostępniający stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązany jest wylogować się z systemu.
19. Przy przetwarzaniu danych osobowych na komputerach przenośnych stosuje się procedury określone powyżej. Pracownicy korzystający z komputerów przenośnych zobowiązani są do ochrony ich przed kradzieżą i dostępem osób nieuprawnionych.

XII. Procedura zabezpieczenia systemu informatycznego

1. Na każdej stacji roboczej, komputerze przenośnym i serwerze musi być zainstalowane oprogramowanie antywirusowe, które sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.
2. Każdy e-mail oraz załączniki muszą być sprawdzone przez program antywirusowy pod kątem obecności wirusów.
3. Definicje wzorców wirusów aktualizowane są nie rzadziej niż raz w miesiącu.
4. Jeżeli oprogramowanie antywirusowe pozwala, to należy ustawić harmonogram zadań tak, aby przynajmniej raz w tygodniu sprawdzał daną jednostkę komputerową pod kątem obecności wirusów.
5. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje pracownik, który pobrał plik.
6. Przeprowadza się cyklicznie kontrole antywirusowe na wszystkich komputerach – minimum co 3 miesiące.
7. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku stwierdzenia nieprawidłowości, zgłoszonych przez pracownika, w funkcjonowaniu sprzętu komputerowego lub oprogramowania.

8. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe, na którym wykryto wirusa, oraz wszystkie posiadane przez pracownika nośniki.
9. Pracownicy mogą korzystać z zewnętrznych nośników danych tylko po uprzednim sprawdzeniu zawartości nośnika oprogramowaniem antywirusowym. Sprawdzenia dokonuje pracownik, który nośnik zamierza użyć.
10. Dostęp do Internetu możliwy jest na wszystkich stacjach roboczych, sieć wewnętrzna jest chroniona centralnym urządzeniem sprzętowym z wbudowanym firewall.
11. System rejestruje datę wprowadzenia danych do systemu.

XIII. Procedura tworzenia kopii zapasowych

1. IOD w porozumieniu z Administratorem wyznacza osobę odpowiedzialną za tworzenie i przechowywanie u Administratora kopii zapasowych przetwarzanych danych osobowych.
2. Kopie zapasowe danych osobowych wykonywane są codziennie, w sposób automatyczny i zawierają pełny obraz danych osobowych.
3. Kopie zapasowe przechowuje się w miejscach odpowiednio zabezpieczonych przed dostępem osób nieuprawnionych w innych pomieszczeniach niż serwerownia przez okres minimum trzech miesięcy.
4. Kopie zapasowe testuje się okresowo, nie rzadziej niż co pół roku.
5. Kopie zapasowe danych osobowych przetwarzanych po ustaniu ich użyteczności są bezzwłocznie usuwane.
6. Kopie zapasowe przetwarzanych danych osobowych, które uległy uszkodzeniu, podlegają natychmiastowemu zniszczeniu.
7. Dostęp do kopii zapasowych posiada ADO, IOD oraz osoba odpowiedzialna za ich tworzenie.
8. Użytkownicy stacji roboczej są zobowiązani do samodzielnego wykonywania kopii zapasowych danych osobowych zapisanych na dysku stacji roboczej.
9. Bezwzględnie zabronione jest samodzielne dokonywanie przez pracowników napraw sprzętu informatycznego, wymiana jego podzespołów oraz wykonywanie innych czynności nie związanych bezpośrednio z jego eksploatacją lub nie dopuszczonych do wykonywania przez producenta sprzętu w instrukcji obsługi.
10. Pracownik ma obowiązek niezwłocznie powiadomić ADO o wszelkich nieprawidłowościach i awariach sprzętu informatycznego, mogących prowadzić do próby naruszenia lub naruszenia bezpieczeństwa danych osobowych.

XIV. Procedura przechowywania elektronicznych nośników informacji

1. Nośniki danych osobowych są przechowywane w sposób uniemożliwiający dostęp do nich osób nieuprawnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych).

2. Dane osobowe w postaci elektronicznej – zapisywane na przenośnych nośnikach danych oraz komputery przenośne mogą być wynoszone poza siedzibę Administratora wyłącznie za wyraźną zgodą Administratora lub IOD.
3. Po zakończeniu pracy przez pracowników wymienne elektroniczne nośniki informacji są przechowywane w zamykanych szafach biurowych.
4. Pracownicy są zobowiązani do niezwłocznego i trwałego usuwania danych osobowych z nośników informacji po ustaniu powodu ich przechowywania.
5. Za bezpieczeństwo danych zapisanych w komputerach przenośnych oraz w innych urządzeniach przenośnych w całości odpowiada użytkownik komputera lub urządzenia przenośnego.
6. W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnętrznego, pracownik jest zobowiązany do sprawdzenia go programem antywirusowym na swoim komputerze.
7. W przypadku konieczności przechowywania wydruków zawierających dane osobowe, należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym.
8. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

XV. Monitoring – ADO jako Pracodawca

W przypadku wprowadzenia monitoringu ADO - pracodawca oznacza pomieszczenia i teren monitorowany w sposób widoczny i czytelny, za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych, nie później niż jeden dzień przed jego uruchomieniem.

Cele, zakres oraz sposób zastosowania monitoringu ustala się w układzie zbiorowym pracy lub w regulaminie pracy albo w obwieszczeniu, jeżeli pracodawca nie jest objęty układem zbiorowym pracy lub nie jest obowiązany do ustalenia regulaminu pracy. Pracodawca przed dopuszczeniem pracownika do pracy przekazuje mu na piśmie informacje dotyczące celu oraz zakresy monitoringu.

Pracodawca informuje pracowników o wprowadzeniu monitoringu, w sposób przyjęty u danego pracodawcy, nie później niż 2 tygodnie przed jego uruchomieniem.

ADO dba o bezpieczeństwo nagrań (zabezpiecza je przed niepowołanym dostępem).

Nagrania obrazu ADO przetwarza wyłącznie do celów, dla których zostały zebrane i przechowuje przez okres nieprzekraczający 3 miesięcy od dnia nagrania a następnie trwale usuwa.

W miejscach objętych monitoringiem zamieszczone są skrócone klauzule informacyjne o treści, których wzór stanowi załącznik do Polityki (**Załącznik nr 24 Wzór: Skrócony Obowiązek Informacyjny – monitoring)**.
W przypadku, gdy osoba wystąpi o przekazanie pełnej informacji, informacja ta powinna zostać przekazana zgodnie ze wzorem, który stanowi załącznik do Polityki (**Załącznik nr 25 Wzór: Obowiązek Informacyjny – monitoring**).

XVI. Procedura ochrony danych osobowych w przypadku połączeń telefonicznych

Osobom kontaktującym się z Administratorem telefonicznie informacje na temat ochrony danych osobowych przekazywane są zgodnie z procedurą, której wzór stanowi załącznik do Polityki (**Załącznik nr 22 Wzór: Procedura ochrony danych osobowych w przypadku połączeń telefonicznych)**.

XVII. Procedura dostępu fizycznego do pomieszczeń

1. Obszar przetwarzania danych jest zabezpieczony przed dostępem osób nieupoważnionych poprzez zastosowanie zamków patentowych.
2. Klucze do pomieszczeń, w których przetwarzane są dane osobowe, jak również do innych zamykanych pomieszczeń , powinny być pobierane, udostępniane i zwracane zgodnie z polityką kluczy, która stanowi załącznik do Polityki.

XVIII. Procedura udostępnienia danych

1. Dane osobowe udostępnia się na pisemny wniosek, chyba że przepis innej ustawy stanowi inaczej.
2. W przypadku wniosku o udostępnienie danych, każda osoba, do której wpłynie taki wniosek, a która ma uzasadnione wątpliwości czy udostępnienie danych będzie zgodne z przepisami prawa, jest zobowiązana przekazać wniosek do IOD.
3. IOD rozpatruje przekazany wniosek oraz ustala czy wniosek o udostępnienie:
    a) Jest sporządzony w formie pisemnej;
    b) Wystarczająco identyfikuje osobę, której dane mają być udostępnione;
    c) Wskazuje odpowiednią podstawę prawną udostępnienia danych;

d) Określa zakres danych osobowych, których wniosek o udostępnienie danych osobowych dotyczy.

4. IOD ocenia, czy można legalnie udostępnić dane osobowe i podejmuje decyzję, którą następnie Administrator przekazuje odbiorcy wniosku.
5. W razie braków formalnych wniosku o udostępnienie danych osobowych, Administrator zwraca się do wnioskodawcy o ich usunięcie we wskazanym terminie pod rygorem pozostawienia wniosku bez rozpoznania.
6. Po uzyskaniu pozytywnej opinii od IOD w przedmiocie dopuszczalności udostępnienia danych osobowych, Administrator bez zbędnej zwłoki udostępnia dane osobowe.
7. Dane osobowe powinny być udostępnione w sposób zapewniający ich poufność wobec osób postronnych.
8. Po uzyskaniu negatywnej opinii od IOD w przedmiocie dopuszczalności udostępnienia danych osobowych, Administrator nie udostępnia danych osobowych.

XIX. Procedura powierzania przetwarzania danych osobowych

1. Administrator korzysta z usług podmiotów przetwarzających, którzy zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO oraz chroniło prawa osób, których dane dotyczą.
2. Administrator dokłada należytej staranności, by przetwarzanie danych osobowych przez podmiot przetwarzający odbywało się na podstawie pisemnej umowy między Administratorem a podmiotem przetwarzającym, której wzór stanowi załącznik do Polityki.
3. Podmiot przetwarzający, któremu Administrator powierzył przetwarzanie danych osobowych, nie może korzystać z usług innego podmiotu przetwarzającego bez uprzedniej pisemnej zgody Administratora.
4. W umowie powierzenia przetwarzania danych osobowych należy zastrzec, że podmiot przetwarzający ma obowiązek poinformować Administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym Administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.
5. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy, która określa przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa Administratora.
6. Umowa powierzenia przetwarzania danych osobowych stanowi w szczególności, że podmiot przetwarzający:
    a) Przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;

b) Zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
c) Podejmuje wszelkie środki by uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku;
d) Przestrzega warunków korzystania z usług innego podmiotu przetwarzającego;
e) Biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw;
f) Uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga Administratorowi wywiązać się z obowiązków nałożonych na Administratora w RODO;
g) Po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji Administratora usuwa lub zwraca Administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo nakazuje przechowywanie danych osobowych;
h) Udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w umowie oraz umożliwia Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

7. Jeżeli do wykonania w imieniu Administratora konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający na mocy umowy powinny zostać nałożone te same obowiązki ochrony danych jak w umowie między Administratorem a podmiotem przetwarzającym.
8. Jeżeli inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego powinna spoczywać na pierwotnym podmiocie przetwarzającym.

XX. Procedura przeprowadzania szkoleń pracowniczych

1. Każda osoba upoważniona do przetwarzania danych osobowych, przed dopuszczeniem do pracy, jest poddawana szkoleniu z zakresu zasad bezpieczeństwa przetwarzania danych

osobowych wynikających z bezwzględnie obowiązujących przepisów prawa oraz niniejszej Polityki.

2. IOD w porozumieniu z Administratorem przeprowadza cykliczne szkolenia pracowników, którzy przetwarzają dane osobowe.
3. Pracownicy potwierdzają swój udział w szkoleniu własnoręcznym podpisem na liście obecności.

4. Ewidencję szkoleń pracowników prowadzi i przechowuje IOD.

XXI. Procedura zgłaszania incydentów

1. W każdym przypadku stwierdzenia naruszenia ochrony danych – także wówczas gdy naruszenie nie skutkuje powstaniem obowiązku zgłoszenia, o którym mowa w pkt. 2 poniżej lub zgłoszenia, o którym mowa w pkt. 3 poniżej – Administrator, zgodnie z art. 33 ust. 5 RODO, dokumentuje okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta ma na celu umożliwienie organowi nadzorczemu weryfikowanie przestrzegania przepisów dotyczących zgłaszania naruszeń. Wzór dokumentacji rejestru naruszeń wskazany został w załączniku do niniejszej Polityki.
2. Wewnętrzny rejestru naruszeń prowadzony jest przez IOD.
3. Zgodnie z art. 33 ust. 1 RODO, w przypadku naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Osobą odpowiedzialną za zgłoszenie jest IOD. Wzór zgłoszenia w sprawie naruszenia ochrony danych osobowych do Prezesa Urzędu Ochrony Danych Osobowych stanowi załącznik do Polityki.
4. Zgłoszenie, o którym mowa w pkt. 3, zawiera co najmniej:
    a) Opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazanie kategorii i przybliżoną liczbę osób, których dane dotyczą, oraz kategorii i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
    b) Imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
    c) Opis możliwych konsekwencji naruszenia ochrony danych osobowych;
    d) Opisy środków zastosowanych lub proponowanych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach opis środków w celu zminimalizowania ewentualnych negatywnych skutków naruszenia.
5. Administrator ma obowiązek poinformować IOD o przypadku naruszenia ochrony danych

osobowych bądź podejrzeniu naruszenia niezwłocznie jednak nie później niż 24 godzin od jego wykrycia. Wzór zgłoszenia w sprawie naruszenia ochrony danych osobowych do IOD stanowi załącznik do Polityki.

6. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Mówiąc o ryzyku naruszenia praw i wolności osób fizycznych na gruncie RODO, konieczne jest uwzględnienie powagi incydentu, tj. wielkości szkody, jakie incydent może spowodować w odniesieniu do osoby, której dane dotyczą. Wzór zawiadomienia osoby zawarty został w załączniku do Polityki.
7. Zawiadomienie osoby, której dane dotyczą powinno być sformułowane jasnym i prostym językiem i powinno opisywać charakter naruszenia ochrony danych osobowych oraz zawierać co najmniej następujące informacje: imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji, opisywać możliwe konsekwencje naruszenia ochrony danych osobowych, opisywać środki zastosowane lub proponowane przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
5. Ocenę prawdopodobieństwa wystąpienia ryzyka naruszenia praw lub wolności człowieka na potrzeby decyzji o konieczności dokonania zgłoszeń, o których mowa w pkt. 2 i 3 powyżej dokonuje IOD w porozumieniu z Administratorem w oparciu o obiektywne kryteria. Analizując możliwe zagrożenia dla podmiotu danych należy uwzględnić w szczególności utratę kontroli nad własnymi danymi osobowymi, dyskryminację, negatywne konsekwencje wizerunkowe, kradzież tożsamości, straty finansowe, czy naruszenie tajemnicy zawodowej.
6. Ryzyko naruszenia praw i wolności może wynikać w szczególności z:
    a) Przetwarzania danych osobowych mogącego prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych,
    b) Przetwarzania mogącego poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową lub wszelką inną znaczną szkodą gospodarczą lub społeczną,
    c) Prawdopodobieństwa, że osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi;
    d) Faktu przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności,
    e) Faktu oceniania czynników osobowych, w szczególności analizowania lub prognozowania aspektów dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia,

osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych,

f) Faktu przetwarzania danych osobowych osób wymagających szczególnej opieki, w szczególności dzieci,

g) Przetwarzania dużej ilości danych osobowych i wpływania na dużą liczbę osób, których dane dotyczą.

7. Zawiadomienie nie jest wymagane, w następujących przypadkach:

a) Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

b) Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;

c) Wymagałoby ono niewspółmiernie dużego wysiłku - takim przypadku Administrator wyda publiczny komunikat lub zastosuje podobny środek, za pomocą którego osoby, których dane dotyczą, zostaną poinformowane w równie skuteczny sposób.

XXII. Regularne testowanie. Ponowna ocena ryzyka. Postępowanie na wypadek zagrożenia bezpieczeństwa danych osobowych. Postępowanie w razie klęski żywiołowej

Regularne testowanie

Administrator regularnie, jednak nie rzadziej niż raz na 12 miesięcy zleca testowanie i weryfikowanie zabezpieczeń stosowanych w zakresie ochrony danych osobowych – w celu wychwycenia ewentualnych luk.

Przedmiotem kontroli powinno być w szczególności:

1. Funkcjonowanie zabezpieczeń systemowych.
2. Prawidłowe funkcjonowanie mechanizmów kontroli dostępu do danych osobowych.
3. Funkcjonowanie zastosowanych zabezpieczeń fizycznych.
4. Zasady przechowywania danych w formie papierowej.
5. Zasady i sposoby archiwizowania oraz likwidacji danych archiwalnych.
6. Realizacja procedur Polityki w zakresie ochrony danych.

IOD regularnie sprawdza aktualność Polityki oraz weryfikuje jej zapisy z praktyką.

Ponowna ocena ryzyka.

Niezależnie od regularnej oceny ryzyka w zakresie ochrony danych osobowych (nie rzadziej niż raz na

12 miesięcy), IOD przeprowadza ocenę ryzyka po każdorazowym wystąpieniu incydentu oraz każdorazowej zmianie mogącej wpływać na poziom ryzyka, w tym szczególnie zmianie struktury organizacyjnej, otoczenia dotyczącego realizacji umów z nowymi podmiotami, technologii, infrastruktury, pracowników, metod pracy lub przepisów prawa.

Postępowanie na wypadek zagrożenia bezpieczeństwa danych osobowych.

Naruszenie ochrony danych osobowych stanowi w szczególności:

1. Nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują,
2. Wszelkie modyfikacje danych osobowych lub próby ich wykonania przez osoby nieuprawnione (np. zmiany zawartości danych, utratę całości lub części danych),
3. Naruszenie lub próby naruszenia integralności systemu informatycznego,
4. Zmianę lub utratę danych na kopiach zapasowych,
5. Naruszenie lub próby naruszenia poufności danych lub ich części,
6. Nieuprawniony dostęp (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu),
7. Udostępnienie osobom nieupoważnionym danych osobowych lub ich części,
8. Zniszczenie, uszkodzenie lub wszelkie próby nieuprawnionej ingerencji w systemy informatyczne zmierzające do zakłócenia ich działania bądź pozyskania w sposób niedozwolony (lub w celach niezgodnych z przeznaczeniem) danych zawartych w systemach informatycznych lub w formie papierowej,
9. Inny stan systemu informatycznego lub pomieszczeń niż pozostawiony przez użytkownika po zakończeniu pracy,
10. Włamanie do budynku lub pomieszczeń, w których przetwarzane są dane osobowe lub próby takich działań.

<u>Do czasu przybycia IOD lub upoważnionej przez IOD osoby, zgłaszający:</u>

1. Powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów.
2. Zabezpiecza elementy systemu informatycznego lub dokumentacji w formie papierowej, przede wszystkim poprzez uniemożliwienie dostępu do nich osób nieupoważnionych.
3. Podejmuje, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.
4. Postanowienia powyższe mają zastosowanie zarówno w przypadku naruszenia, jak i w przypadku podejrzenia naruszenia danych osobowych.

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie ochrony danych osobowych IOD lub osoba przez niego upoważniona, po przybyciu na miejsce:

1. Ocenia zaistniałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane oraz stan urządzeń, a także identyfikuje wielkość negatywnych następstw incydentu.
2. Wysłuchuje relacji osoby, która dokonała powiadomienia.
3. W porozumieniu z Administratorem podejmuje decyzję o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych.

Postępowanie w razie klęski żywiołowej

1. Klęską żywiołową jest katastrofa, spowodowana działaniem sił przyrody takich jak ogień, woda, huragan, lub ich przejawami.
2. W przypadku wystąpienia zagrożenia powodującego konieczność przeprowadzenia ewakuacji osób lub mienia z pomieszczeń, w których przetwarzane są dane osobowe, mają zastosowanie przepisy niniejszego rozdziału oraz innych przepisów szczególnych.
3. Osoby biorące udział w akcji ratunkowej, mają prawo wejść do pomieszczeń w których przetwarzane są dane osobowe.
4. W przypadku ogłoszenia alarmu ewakuacyjnego użytkownicy, przebywający w pomieszczeniach, w których przetwarzane są dane osobowe, obowiązani są do przerwania pracy, a w miarę możliwości przed opuszczeniem tych pomieszczeń do:
    a) Zamknięcia systemu informatycznego;
    b) Zabezpieczenia danych osobowych znajdujących się w formie papierowej.
5. W czasie trwania akcji ratunkowej i po jej zakończeniu pracownicy powinni, w miarę możliwości, zabezpieczyć dane osobowe przed nieuprawnionym do nich dostępem. Obowiązek ten ciąży w równym stopniu na wszystkich pracownikach obecnych przy akcji ratunkowej.

XXIII. Postanowienia końcowe

1. Polityka jest dokumentem wewnętrznym i osoby, które uzyskały wgląd w jej treść, zobowiązane są do zachowania jej w poufności.
2. Przypadki nieuzasadnionego zaniechania obowiązków określonych w niniejszym dokumencie traktowane będą jako ciężkie naruszenie podstawowych obowiązków pracowniczych.
3. W sprawach nieuregulowanych w niniejszej Polityce ochrony danych mają zastosowanie przepisy 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 oraz inne przepisy

prawa z zakresu ochrony danych osobowych, a także inne przepisy z zakresu ochrony danych osobowych.

XXIV. Pojęcia z zakresu ochrony danych osobowych

Pojęcie	Znaczenie
Adekwatność Lub Minimalizacja danych	Zasada dotycząca przetwarzania danych osobowych polegająca na tym, że Administrator danych powinien przetwarzać tylko takiego rodzaju dane i tylko o takiej treści, które są niezbędne do realizacji celu dla którego dane są zbierane;
Administrator	Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. W niniejszej dokumentacji ochrony danych osobowych przez Administratora danych rozumie się Zespół Szkół w Gołaszynie, adres: Gołaszyn 29, 21-400 Łuków;
Analiza ryzyka	Proces identyfikacji ryzyka, określania jego wartości i identyfikowanie niezbędnych zabezpieczeń;
Anonimizacja	Przekształcenie danych osobowych, po którym nie można już przyporządkować poszczególnych informacji osobistych lub rzeczowych do określonej lub możliwej do zidentyfikowania osoby fizycznej albo można tego dokonać jedynie niewspółmiernie dużym nakładem czasu, kosztów lub działań;
Audyt zgodności	Czynności mające na celu zweryfikowanie zgodności przetwarzania danych osobowych z przepisami RODO oraz innymi przepisami o ochronie danych osobowych, a także czynności mające na celu monitorowanie przestrzegania Polityki ochrony danych osobowych;
Dane biometryczne	Dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;
Dane dotyczące zdrowia	Dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej, w tym o korzystaniu z usług opieki zdrowotnej, ujawniające informacje o stanie jej zdrowia;
Dane genetyczne	Dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;
Dane osobowe	Informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba

	fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
Dostępność	Właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu;
Działania zaradcze	Środki zastosowane lub proponowane przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym środki w celu zminimalizowania ewentualnych negatywnych skutków naruszenia;
Hasło	Ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
Identyfikator	Ciąg znaków literowych, cyfrowych lub innych znaków identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
Incydent	Naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
Integralność	Zasada dotycząca przetwarzania danych osobowych zapewniająca, że dane nie zostały zmienione, dodane lub usunięte w nieautoryzowany sposób;
IOD	Osoba pełniąca funkcję inspektora ochrony danych w rozumieniu art. 37 RODO;
Istotność ryzyka	Iloczyn prawdopodobieństwa i wpływu ryzyka określający potencjalny skumulowany poziom wpływu ryzyka na osiąganie przez Administratora zamierzonych celów;
Legalność	Zasada dotycząca przetwarzania danych osobowych zapewniająca, że dane osobowe są przetwarzane zgodnie z prawem, po spełnieniu przynajmniej jednego z warunków określonych w art. 6 ust. 1 lub art. 9 ust. 2 RODO;
Odbiorca	Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Przy czym odbiorcą nie jest organ publiczny, który może otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem unii europejskiej lub prawem państw członkowskiego;

Ograniczenie celu	Zasada dotycząca przetwarzania danych osobowych zapewniająca, że dane osobowe są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
Okresowość	Zasada dotycząca przetwarzania danych osobowych zapewniająca, że dane osobowe są przetwarzane przez okres nie dłuższy, niż jest to niezbędne do celów, dla realizacji których dane są przetwarzane;
Organ nadzorczy	Niezależny organ publiczny powołany w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych w unii europejskiej, zgodnie z art. 51 RODO;
Osoba upoważniona	Osoba upoważniona przez Administratora do przetwarzania danych osobowych, nad którą Administrator sprawuje bezpośrednią kontrolę w procesie przetwarzania danych realizowanym przez tę osobę;
Podmiot przetwarzający	Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;
Polityka	Niniejszy dokument, tj. Polityka ochrony danych;
Poufność	Właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom;
Pracownik Lub Współpracownik	Osoba zatrudniona przez Administratora na podstawie umowy o pracę oraz osoba świadcząca na rzecz Administratora usługi na podstawie umów cywilnoprawnych, a także praktykanci, wolontariusze, stażyści i studenci;
Przetwarzanie	Operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
Pseudonimizacja	Przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

Raport z audytu	Dokument opracowywany przez zespół Inspektora Ochrony Danych po dokonaniu audytu zgodności zawierający opis niezgodności przetwarzania danych osobowych z przepisami RODO, innymi przepisami o ochronie danych osobowych oraz Polityką, a także zawierający ogólną ocenę poziomu ochrony danych osobowych u Administratora;
Rejestr czynności przetwarzania danych osobowych	Dokument, o którym mowa w art. 30 ust. 1 RODO, prowadzony w formie pisemnej przez Administratora, udostępniany organowi nadzorczemu na jego żądanie;
Rejestr wszystkich Kategorii czynności przetwarzania	Dokument, o którym mowa w art. 30 ust. 2 RODO, prowadzony w formie pisemnej przez podmiot przetwarzając, udostępniany organowi nadzorczemu na jego żądanie;
RODO	Rozporządzenie parlamentu europejskiego i rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. W sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/we (ogólne rozporządzenie o ochronie danych);
Rozliczalność przetwarzania	Właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
Ryzyko	Kombinacja prawdopodobieństwa zdarzenia i jego konsekwencji. Ryzyko związane z bezpieczeństwem danych osobowych to prawdopodobieństwo, że określone zagrożenie wykorzysta podatność zasobu lub grupy zasobów, aby spowodować straty lub zniszczenie zasobów;
Rzetelność	Zasada dotycząca przetwarzania danych osobowych zapewniająca merytoryczną poprawność danych osobowych poprzez ich zgodność ze stanem faktycznym, kompletność i aktualność;
Strona trzecia lub osoba trzecia	Osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, Administrator, podmiot przetwarzający czy osoby, które – z upoważnienia Administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;
System informatyczny	Zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
Upoważnienie	Oświadczenie nadane przez Administratora wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w tym oświadczeniu, nad którą Administrator sprawuje bezpośrednią kontrolę w procesie przetwarzania danych realizowanym przez tę osobę;

Uwierzytelnianie	Działanie, którego celem jest weryfikacja deklarowanej tożsamości osoby upoważnionej;
Zabezpieczenie	Środki służące zarządzaniu ryzykiem, łącznie z politykami, procedurami, zaleceniami, praktyką lub strukturami organizacyjnymi, które mogą mieć naturę Administracyjną, techniczną, zarządczą lub prawną;
Zagrożenie	Niepożądane zdarzenie, które powoduje, że ryzyko materializuje się w postaci wymiernej straty poprzez wystawienie danych osobowych na utratę, ujawnienie, zniszczenie lub zmianę;
Zarządzanie ryzykiem	Skoordynowane działania w celu identyfikacji, minimalizacji lub eliminacji prawdopodobieństwa oraz skutków realizacji zagrożeń;
Zbiór danych	Uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;