Zarządzenie nr SP4.021.30.2019

Dyrektora Szkoły Podstawowej nr 4 w Radlinie

z dnia 03 grudnia 2019r.

w sprawie: wprowadzenia Polityki Ochrony Danych.

Podstawa prawna: Na podstawie artykułu 24 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE,

zarządza, co następuje:

§1.

W celu zapewnienia ochrony danych, w tym danych osobowych, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych w zakresie ochrony danych, wprowadzam do stosowania w Szkole Podstawowej Nr 4 im. Gustawa Morcinka w Radlinie **„Politykę Ochrony Danych”,** w brzmieniu ustalonym w załączniki do niniejszego Zarządzenia.

§2.

Nadzór nad wykonaniem zarządzenia powierzam Dyrektorowi Szkoły.

§3.

Zarządzenie wchodzi w życie z dniem podpisania.

§ 4.

Zarządzenie podlega ogłoszeniu na stronie internetowej szkoły www.sp4.radlin.pl i w księdze zarządzeń.

Dyrektor szkoły
mgr Małgorzata Mokrosz

Załącznik do Zarządzenia nr SP4.021.30.2019
z dnia 3 grudnia 2019 r.
w sprawie wprowadzenia
Polityki Ochrony Danych.

POLITYKA OCHRONY DANYCH

ROZDZIAŁ I

Wprowadzenie

§ 1

Cel

Dokument określa zasady dot. ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych, w tym również zasady dot. bezpieczeństwa teleinformatycznego.

§ 2

Definicje

Znaczenie określeń na użytek niniejszego dokumentu:

- **Podmiot Szkoła Podstawowa nr 4 im G. Morcinka**
  z siedzibą w **Radlinie ul Wiosny Ludów 287**
  reprezentowanych przez **mgr Małgorzatę Mokrosz – dyrektora szkoły**
- **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),
- **Administrator** - Administrator danych osobowych w podmiocie określonym w pkt. 1, w rozumieniu art. 4 pkt. 7 RODO,
- **chmura danych** - model przetwarzania oparty na dostarczaniu usług przez podmiot zewnętrzny, polegający na udostępnienie zdalnej infrastruktury informatycznej,
- **dane** lub **dane osobowe** – dane osobowe w rozumieniu art. 4 pkt. 1 RODO,
- **hasło** - ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi,
- **identyfikator** - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę w systemie informatycznym,
- **informacje** – wszelkie dane, w tym również dane osobowe,
- **Inspektor Ochrony Danych** - osoba, której Administrator powierzył pełnienie obowiązków Inspektora Ochrony Danych w podmiocie określonym w pkt. 1, w zakresie określonym w art. 39 ust. 1 RODO,
- **integralność danych** - właściwość zapewniająca, iż dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

- **Koordynator techniczny** – osoba wyznaczona przez Administratora do zarządzania systemami informatycznymi lub do nadzorowania prac dot. zarządzania tymi systemami przez inne podmioty lub osoby oraz do dokumentowania działań w tym zakresie,
- **opiniowanie** – wydawanie opinii; za wydanie opinii pozytywnej, bez uwag, uznaje się również złożenie popisu przez opiniującego pod treścią opiniowanego dokumentu,
- **osoby funkcyjne w zakresie ochrony danych osobowych** - Administrator, Inspektor Ochrony Danych, Koordynator Techniczny oraz wskazany w odrębnym dokumencie Koordynator ds. ochrony danych (zastępujący Inspektora Ochrony Danych),
- **podmiot przetwarzający** - podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawartej zgodnie z art. 28 RODO,
- **Polityka** – niniejszy dokument, tj. „Polityka ochrony danych",
- **poufność danych** - właściwość zapewniająca, iż dane nie są udostępniane nieupoważnionym,
- **pracownik** - osoba świadcząca pracę na podstawie stosunku pracy lub stosunku cywilnoprawnego, w tym również osoba fizyczna, która w ramach prowadzonej działalności gospodarczej wykonuje wyłącznie osobiście, powierzone jej na podstawie umowy cywilnoprawnej zadania; również osoba odbywająca w Podmiocie praktykę lub staż,
- **rozliczalność danych** - właściwość zapewniająca, iż podejmowane działania mogą być przypisane w sposób jednoznaczny konkretnej osobie lub podmiotowi,
- **system informatyczny** - sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych,
- **upoważniony** - osoba, która została upoważniona na piśmie przez Administratora do przetwarzania danych osobowych,
- **uwierzytelnianie** - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości,
- **użytkownik** - upoważniony, któremu nadano identyfikator i przyznano hasło w systemie informatycznym.

§ 3
Zakres stosowania

- Zasady i procedury określone w niniejszym dokumencie stosuje się zarówno do danych osobowych przetwarzanych w sposób tradycyjny w księgach, wykazach, aktach i innych zbiorach, jak i przetwarzanych w systemach informatycznych.
- Zasady i procedury określone w Polityce stosuje się do wszystkich osób zatrudnionych w jednostce, jak i pozostałych osób, które zostały dopuszczone do przetwarzania danych np. praktykantów, stażystów, osób świadczących usługi na podstawie umów cywilnoprawnych.

§ 4
Deklaracje i zobowiązania

- Administrator, świadomy wagi zagrożeń jakie niesie za sobą przetwarzanie danych osobowych dla wolności i praw osób, których dane dotyczą, uznaje ochronę tych danych, za jeden z priorytetów swojej działalności.
- Administrator, podejmuje działania mające na celu zapewnienie stałej zgodności realizowanych zdań z przepisami i dobrymi praktykami dot. ochrony danych osobowych.
- Administrator, deklaruje, że niniejszy dokument stanowi politykę ochrony danych w rozumieniu art. 24 ust. 2 RODO.
- Administrator, świadomy zagrożeń względem systemów informatycznych, uznaje ochronę przed tymi zagrożeniami za kolejny priorytet swojej działalności. Mając na uwadze, iż na informacje przetwarzane w systemach informatycznych składają się również dane osobowe, należy założyć, że poprzez ochronę danych osobowych przetwarzanych w tych systemach pośrednio zapewniona zostaje również ochrona pozostałych przetwarzanych w ten sposób informacji.
- Administrator, zobowiązuje wszystkie osoby dopuszczone przez siebie do przetwarzania danych osobowych do dostosowania ich postępowania do wymogów wynikających z niniejszej Polityki, innych uregulowań wewnętrznych dot. ochrony danych, wypracowanych w Podmiocie zasad zwyczajowych i dobrych praktyk.

ROZDZIAŁ II
Role i odpowiedzialności

§ 5
Administrator

Administrator realizuje zadania w zakresie ochrony danych osobowych, w tym w szczególności:

- podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, zmian w strukturze Podmiotu oraz zmian w technikach zabezpieczenia danych osobowych,
- zapewnia odpowiednie do zagrożeń środki techniczne i rozwiązania organizacyjne,
- wyznacza Inspektora Ochrony Danych oraz zapewnia kontrolę i nadzór nad przetwarzaniem danych osobowych,
- upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi ich obowiązków,
- podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych,
- wdraża wszystkie niezbędne dokumenty wynikające z zapisów RODO oraz innych aktów prawnych mających zastosowanie przy przetwarzaniu danych osobowych.

§ 6

Inspektor Ochrony Danych

Inspektor Ochrony Danych realizuje zadania mu przypisane w RODO i krajowych przepisach prawa dot. ochrony danych osobowych. Udziela opinii dot. dokumentów oraz odpowiednich klauzul w dokumentach dotyczących ochrony danych osobowych, jeżeli nie powoduje to konfliktu interesu, prowadzi lub nadzoruje prowadzenie wybranej dokumentacji z zakresu ochrony danych osobowych. Inspektorowi Ochrony Danych zapewnia

się wsparcie w zakresie realizacji zadań na zasadach uregulowanych odrębnym dokumentem, tj. Zarządzeniem Burmistrza Radlina nr S.0050.0205.2018 z dnia 06 listopada 2018 r. w sprawie wprowadzenia systemu szkoleń wewnętrznych dot. ochrony danych osobowych i wyznaczenia koordynatorów ds. ochrony danych w jednostkach organizacyjnych Miasta Radlin

(wraz z ewentualnymi późniejszymi zmianami).

§ 7

Koordynator Techniczny

Koordynator Techniczny odpowiada za realizację wskazanych w Polityce zadań związanych z elektronicznym przetwarzaniem danych oraz innych zadań dot. obsługi informatycznej wskazanych przez Administratora. Realizacja ww. zadań może być realizowana samodzielnie

przez Koordynatora Technicznego, lub zlecana do wykonania np. innym pracownikom, podmiotom zewnętrznym. W takim przypadku Koordynator Techniczny nadzoruje realizację zadań. Koordynatorem Technicznym w Podmiocie jest pracownik zatrudniony na stanowisku **sekretarka.**

§ 8

Upoważniony

Każdy upoważniony do przetwarzania danych osobowych jest zobowiązany przestrzegać w szczególności następujących zasad:

- może przetwarzać dane osobowe wyłącznie w ustalonym zakresie, na podstawie wydanego przez Administratora upoważnienia i tylko w celu wykonywania nałożonych na niego obowiązków; rozwiązanie stosunku pracy, wygaśnięcie umowy, odwołanie z pełnionej funkcji, powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych,
- musi zachować w tajemnicy treść danych osobowych oraz sposób ich zabezpieczenia; jest zobowiązany do zachowania powyższych tajemnic przez cały okres, również po ustaniu stosunku pracy, wygaśnięciu umowy lub odwołaniu z pełnionej funkcji,
- zapoznaje się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami Polityki i innych procedur wewnętrznych dot. ochrony danych, w zakresie go dotyczącym,
- chroni dane przed ich utratą, nieautoryzowanym zmienieniem lub ujawnieniem osobom nieupoważnionym,
- stosuje się do wydawanych procedur, wytycznych oraz poleceń służbowych mających na celu zapewnienie zgodnego z prawem przetwarzania danych osobowych,
- korzysta w systemów informatycznych w sposób zgodny ze wskazówkami zawartymi w Polityce, instrukcjach oraz instruktażach Koordynatora Technicznego,
- regularnie korzysta z wewnętrznego serwisu informacyjnego https://radlin.type.pl/repozytorium/,
- uczestniczy w szkoleniach z zakresu ochrony danych osobowych na zasadach uregulowanych odrębnym dokumentem, tj. Zarządzeniem Burmistrza Radlina nr S.0050.0205.2018 z dnia 06 listopada 2018 r. w sprawie wprowadzenia systemu szkoleń wewnętrznych dot. ochrony danych osobowych i wyznaczeniu koordynatorów ds. ochrony danych w jednostkach organizacyjnych Miasta Radlin (wraz z ewentualnymi późniejszymi zmianami).

ROZDZIAŁ III
Organizacja

§ 9
Obszary przetwarzania danych

- Dane przetwarzane są w siedzibie Podmiotu, na całym obszarze, bez wyłączenia określonych stref.
- Dane mogą być przetwarzane poza siedzibą Podmiotu, na urządzeniach mobilnych.
- Dane mogą być przetwarzane na odległość poza siedzibą Podmiotu, w tzw. chmurach danych.

§ 10
Zasoby danych osobowych

Wykaz przetwarzanych danych określa Rejestr Czynności Przetwarzania, w formie tzw. „celów przetwarzania", tj. zespołów powiązanych ze sobą operacji na danych, wykonywanych przez jedną lub kilka osób, które można określić w sposób zbiorczy, w związku z celem, w jakim te czynności są podejmowane (tj. czynności przetwarzania).

§ 11
Dokumentacja dot. ochrony danych

Podmiot prowadzi dokumentację ochrony danych osobowych, na którą składają się w szczególności:

- Rejestr Czynności Przetwarzania,
- Rejestr Kategorii Czynności Przetwarzania,
- upoważnienia do przetwarzania danych osobowych (zawierające również oświadczenia osób upoważnionych, zakresy czynności praktykantów i stażystów),
- dokumentację z przeprowadzonych sprawdzeń, kontroli, audytów,
- umowy o powierzeniu przetwarzania danych osobowych,
- umowy o współadministrowaniu,

- porozumienia,
- potwierdzenia odbycia szkoleń przez osoby upoważnione do przetwarzania danych osobowych.

ROZDZIAŁ IV
Zagrożenia bezpieczeństwa danych osobowych i przeciwdziałanie tym zagrożeniom

§ 12
Podstawowe zasady ochrony danych

Przetwarzając dane osobowe, pracownik w sposób szczególny powinien zwracać uwagę na przestrzeganie następujących zasad:

- zasada legalności przetwarzania - należy zapewnić by dane osobowe były przetwarzane wyłącznie po spełnieniu jednego z warunków dopuszczalności przetwarzania,
- zasada przejrzystości przetwarzania - należy zapewnić przejrzystą informację osobom których dane są przetwarzane o dotyczącym ich przetwarzaniu,
- zasada rzetelności przetwarzania - dane powinny być przetwarzane uczciwie w stosunku do osób, których dane są przetwarzane; podejmując dowolne czynności przetwarzania należy brać pod uwagę prawa i interesy osób których dane są przetwarzane; należy wziąć pod uwagę, że przetwarzanie może być dokuczliwe dla tych osób i spróbować zminimalizować te uciążliwości,
- zasada ograniczoności celu - dane wolno zbierać jedynie w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie wolno ich przetwarzać po zebraniu w sposób niezgodny z tymi celami; do celu należy dostosować nie tylko ilość zbieranych danych, ale także zakres ich przetwarzania oraz okres przez który są przechowywane,
- zasada minimalizacji danych - dane powinny być adekwatne do celu, czyli ograniczone do niezbędnego minimum; gdy cel przetwarzania tego nie wymaga to w ogóle nie należy dokonywać identyfikacji osobowej,
- zasada prawidłowość danych - dane powinny być prawdziwe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe,

które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane,

- zasada ograniczenia przechowywania - dane wolno przechowywać w formie umożliwiającej identyfikację osoby, której dane dotyczą, jedynie przez okres niezbędny do realizacji celów, w których dane te są przetwarzane.

§ 13

Identyfikacja zagrożeń bezpieczeństwa danych osobowych

Identyfikuje się w szczególności następujące zagrożenia bezpieczeństwa danych osobowych przetwarzanych w Podmiocie:

- sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych, jak np. pożar, zalanie pomieszczeń, katastrofa budowlana, niepożądana ingerencja ekipy remontowej, włamanie do budynku,
- niewłaściwe parametry środowiska, negatywnie wpływające na dokumentację lub zakłócające pracę urządzeń komputerowych (np. nadmierna wilgotność lub bardzo wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy, wibracje pochodzące

od urządzeń przemysłowych),

- awarie sprzętu lub oprogramowania, zarówno losowe, jak i spowodowane przez niewłaściwe działanie użytkowników i serwisantów,
- zastosowanie niewłaściwych metod zabezpieczenia systemu informatycznego lub brak dostosowania poziomu zabezpieczeń do aktualnego poziomu wyzwań technologicznych,
- działania przestępcze mające na celu przejęcie, zniszczenie lub modyfikację danych osobowych (np. kradzież dokumentów, działanie wirusów i innego szkodliwego oprogramowania, ataki internetowe, wykorzystywanie luk w oprogramowaniu),
- podejmowanie pracy w systemie z przełamaniem lub zaniechaniem stosowania procedur ochrony danych (np. praca osoby, która nie jest upoważniona do przetwarzania, pozostawienie serwisantów bez nadzoru, przyzwolenie na naprawę sprzętu zawierającego dane osobowe poza siedzibą Podmiotu),
- naruszenia zasad i procedur określonych w Polityce przez osoby upoważnione do przetwarzania danych osobowych, będące skutkiem nieprzestrzegania procedur ochrony danych, w tym zwłaszcza

•wprowadzanie zmian do systemu informatycznego,

•instalowanie programów bez wiedzy i zgody Koordynatora Technicznego,

•ujawnienie osobom nieupoważnionym danych osobowych, jak też procedur ochrony danych osobowych stosowanych w Podmiocie (poprzez umożliwienie wglądu lub przekazanie danych i dokumentacji),

•naruszenie bezpieczeństwa danych przez nieautoryzowane ich przetwarzanie lub zgoda na takie działania przez inne osoby (np. udostępnienie identyfikatora i hasła innemu użytkownikowi),

•niezgodne z procedurami zakończenie pracy lub opuszczenie stanowiska pracy (np. nieprawidłowe wyłączenie komputera, niezablokowanie wyświetlenia treści pracy na ekranie komputera przed tymczasowym opuszczeniem stanowiska pracy, pozostawienie po zakończeniu pracy niewłożonych do zamykanych na klucz szaf dokumentów zawierających dane osobowe, niezamknięcie na klucz pokoju po jego opuszczeniu, nieoddanie klucza do pokoju po zakończeniu pracy, niezamknięcie drzwi do budynku lub pozostawienie otwartych okien),

•utratę urządzeń przenośnych lub uzyskanie dostępu do danych zawartych w tych urządzeniach przez osoby nieupoważnione.

§ 14
Techniczne i organizacyjne środki zapewniające ochronę danych

•Stosuje się środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych odpowiednie do zagrożeń, a w szczególności zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

•W podmiocie stosuje się w szczególności następujące środki bezpieczeństwa:

•fizyczne środki ochrony

•wejścia do budynku zabezpieczone są co najmniej drzwiami zwykłymi zamykanymi na klucz,

- dane przechowywane są w pomieszczeniach zabezpieczonych drzwiami zwykłymi zamykanymi na klucz,
- zasoby danych osobowych w formie papierowej przechowywane są w zamkniętych niemetalowych lub metalowych szafach lub innych meblach,
- pomieszczenia, w których przetwarzane są zasoby danych osobowych, zabezpieczone są przed skutkami pożaru za pomocą wolno stojących gaśnic,
- dokumenty zawierające dane osobowe po ustaniu przydatności są stosownie archiwizowane,
- dokumenty zawierające dane osobowe, które nie podlegają archiwizacji, po ich wykorzystaniu są odpowiednio niszczone,
- środki ochrony danych informatycznych
- stosuje się urządzenia typu UPS chroniące systemy informatyczne przed skutkami awarii zasilania,
- dostęp do systemów operacyjnych na stacjach roboczych oraz do systemów dziedzinowych, w których przetwarzane są dane, zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,
- hasła dostępowe do systemów informatycznych są okresowo zmieniane,
- stosuje się oprogramowanie antywirusowe i oprogramowanie ograniczające dostęp typu firewall,
- część sieci informatycznej przeznaczona dla gości, itp. jest w sposób fizyczny lub logiczny oddzielona od części sieci wewnętrznej, gdzie przetwarzane są dane osobowe,
- jeżeli to możliwe, zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika,
- wykonywane są okresowo kopie zapasowe danych,
- organizacyjne środki ochrony
- osoby zatrudnione przy przetwarzaniu danych osobowych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych,
- osoby zatrudnione przy przetwarzaniu danych osobowych zostały zaznajomione w zakresie zabezpieczeń systemów informatycznych,
- osoby zatrudnione przy przetwarzaniu danych osobowych zostały upoważnione do ich przetwarzania i zobowiązane do zachowania ich w tajemnicy,
- określono zakresy odpowiedzialności w zakresie dot. ochrony danych osób funkcyjnych,

•dane osobowe przekazuje się innym podmiotom wyłącznie na podstawie właściwych przesłanek.

§ 15

Zasady upoważniania

•Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora. Zakres upoważnienia określany jest indywidualnie i może obejmować:

•dane osobowe niezbędne do realizacji powierzonych zadań w związku z zawartą umową o pracę, wynikające z zajmowanego stanowiska, określone w regulaminie organizacyjnym Podmiotu oraz indywidualnym zakresie czynności,

•dane osobowe niezbędne do realizacji powierzonych zadań w ramach odbywania praktyki lub stażu, określone w indywidualnym zakresie czynności praktykanta lub stażysty,

•dane osobowe niezbędne do realizacji powierzonych zadań wynikających z zawartej umowy cywilnoprawnej,

•dane należące do szczególnych kategorii danych osobowych lub dane dotyczące wyroków skazujących i naruszeń prawa.

•W podmiocie prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.

•Wszystkie osoby upoważnione do przetwarzania danych osobowych zobowiązane są do zachowania tych danych oraz sposobu ich zabezpieczenia w tajemnicy. Osoby składają oświadczenie następującej lub tożsamej treści:

„Ja niżej podpisany(-a) oświadczam, że:

•*Zapoznałem się z obowiązującymi przepisami dot. ochrony danych danych (w tym w szczególności z Rozporządzeniem Parlamentu Europejskiego i Rady 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 wewnętrznymi regulacjami w tym zakresie (w tym w szczególności Polityką ochrony danych administratora); zapoznałem się z Zasadami Przetwarzania Danych,*

- *zobowiązuję się do zachowania w poufności danych osobowych, do których uzyskam dostęp w związku z wykonywaniem powierzonych mi czynności, w tym również do zapewnienia bezpieczeństwa tych danych, ochrony przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz ich przypadkową utratą, zniszczeniem lub uszkodzeniem, itp.,*
- *zobowiązuję się do zachowania w tajemnicy organizacyjnych i technicznych sposobów zabezpieczenia danych osobowych,*
- *zobowiązuję się do zachowania poufności w zakresie wskazanym w pkt. 2 i 3 również po zakończeniu realizacji powierzonych mi czynności, zmianie stanowiska, ustaniu stosunku pracy, rozwiązaniu lub wygaśnięciu innego stosunku prawnego,*
- *zobowiązuję się do niezwłocznego poinformowania kierownika jednostki (administratora danych osobowych) o fakcie wejścia w posiadanie danych osobowych, co do przetwarzania których nie zostałem(-am) upoważniony(-a),*
- *przyjmuję do wiadomości, iż za postępowanie niezgodne z powyższymi zobowiązaniami mogę zostać pociągnięty(-a) do odpowiedzialności, w szczególności dyscyplinarnej i karnej,*
- *przyjmuję do wiadomości, że w związku z zapewnieniem bezpieczeństwa, pracodawca zastrzega sobie prawo do monitorowania i archiwizacji służbowej poczty elektronicznej oraz danych zapisanych na urządzeniach służbowych oraz do monitorowania połączeń internetowych i telefonicznych."*

- Ryzyko naruszenia zasad ochrony danych osobowych ze strony osób, które nie zostały upoważnione do przetwarzania danych osobowych (np. personel sprzątający) minimalizuje się przez odpowiednie ich pouczenie oraz zobowiązanie do zachowania w tajemnicy danych osobowych, o których powzięli wiedzę w sposób przypadkowy oraz sposobu ich zabezpieczenia. Osoby składają oświadczenie następującej lub tożsamej treści:

„Ja niżej podpisany(-a) oświadczam, że:
- *zobowiązuję się do zachowania w poufności danych osobowych, do których uzyskam dostęp, w tym również do zapewnienia bezpieczeństwa tych danych; zobowiązuję się do niezwłocznego poinformowania kierownika jednostki (administratora danych*

osobowych) o fakcie wejścia w posiadanie danych osobowych, co do przetwarzania których nie zostałem(-am) upoważniony(-a),

- *zobowiązuję się do zachowania w tajemnicy organizacyjnych i technicznych sposobów zabezpieczenia danych osobowych,*
- *zobowiązuję się do zachowania poufności w zakresie wskazanym w pkt. 1 i 2 również po zakończeniu realizacji powierzonych mi czynności, zmianie stanowiska, ustaniu stosunku pracy, rozwiązaniu lub wygaśnięciu innego stosunku prawnego,*
- *przyjmuję do wiadomości, iż za postępowanie niezgodne z powyższymi zobowiązaniami mogę zostać pociągnięty(-a) do odpowiedzialności."*

§ 16

Ogólne zasady postępowania pracowników

Pracownicy zobowiązani są do zachowania w szczególności następujących reguł bezpieczeństwa:

- zachowania danych osobowych i sposobu ich zabezpieczenia w tajemnicy, w tym także wobec osób najbliższych,
- przestrzegania indywidualnych uprawnień i realizacji obowiązków w zakresie przetwarzania danych osobowych, w tym właściwego korzystania z powierzonych sprzętów i udostępnionych zasobów oraz używania wyłącznie własnego identyfikatora i hasła,
- niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych,
- powstrzymywania się od samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu oraz instalowania nieautoryzowanego oprogramowania, nawet gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych,
- niepozostawiania bez kontroli włączonych urządzeń zawierających dane osobowe oraz niezabezpieczonych dokumentów,
- dbania o prawidłową wentylację komputerów,
- niepodłączania do gniazd i listew zasilających przeznaczonych dla sprzętu komputerowego innych urządzeń, szczególnie łatwo powodujących zwarcia lub przeciążenia (np. grzejniki, czajniki, wentylatory),

•odpowiedniego zabezpieczenia hasła wymaganego do uwierzytelnienia się w systemie informatycznym oraz nieudostępniania go innym osobom,
•ustawiania ekranów komputerowych tak, by osoby nieuprawnione nie widziały treści wyświetlanych na ekranie,
•zamykania okien w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu sprzętu komputerowego lub bezpieczeństwu dokumentów,
•zapisywania plików lub wykonywania kopii roboczych danych, na których się właśnie pracuje, tak często jak to możliwe, aby zapobiec ich utracie,
•kasowania z przenośnych nośników danych, plików po ich wykorzystaniu,
•niszczenia przy użyciu niszczarki niepotrzebnych wydruków i kopii dokumentów po ich wykorzystaniu,
•dbanie o odpowiednie zabezpieczenie wszelkich dokumentów i wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy (np. w szafie zamykanej na klucz),
•umieszczania kluczy do szaf (mebli) w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy,
•zamykania okien w razie opuszczania pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy,
•zamykania drzwi na klucz po zakończeniu pracy w danym dniu i złożenia klucza w wyznaczonym miejscu (zabronione jest pozostawianie kluczy w drzwiach do pomieszczenia, w którym przetwarzane są dane osobowe).

§ 17
Praca poza siedzibą Podmiotu

•Wynoszenie poza siedzibę Podmiotu dokumentów, nośników danych (plików) i urządzeń zawierających dane osobowe oraz telepraca polegająca na świadczeniu pracy spoza siedziby Podmiotu są dopuszczalne jedynie za wiedzą i zgodą Administratora.
•Koordynator Techniczny prowadzi rejestr urządzeń (komputerów, tabletów, telefonów) wynoszonych poza siedzibę Podmiotu i osób z nich korzystających oraz osób podejmujących telepracę.
•Dokumenty, nośniki danych i urządzenia zawierające dane osobowe wynoszone poza siedzibę Podmiotu należy chronić przed uszkodzeniami.

- Podejmując telepracę należy stosować wymagane zabezpieczenia.
- Dokumenty, nośniki danych oraz urządzenia wynoszone poza siedzibę Podmiotu nie mogą być pozostawiane bez nadzoru. Zabronione jest również pozostawianie ich bez nadzoru w samochodach, przechowalniach bagażu, zamykanych schowkach w miejscach publicznych, itp..
- Wykorzystywanie dokumentów, nośników danych oraz urządzeń zawierających dane osobowe w miejscach publicznych jest dozwolone, o ile otoczenie, w którym znajduje się osoba upoważniona do przetwarzania danych osobowych, stwarza warunki minimalizujące ryzyko utraty, zniszczenia lub zapoznania się z danymi przez osoby nieupoważnione.
- Niedozwolone jest udostępnianie dokumentów, nośników danych i urządzeń osobom nieupoważnionym, w tym domownikom i osobom bliskim użytkownika.
- Obowiązuje zakaz samodzielnej instalacji oprogramowania i modernizacji podzespołów w powierzonych urządzeniach, bez udziału Koordynatora Technicznego. Zakaz samodzielnej instalacji oprogramowania nie obowiązuje, jeżeli na powierzonym urządzeniu nie znajdują się służbowe dane osobowe.
- Obowiązuje zakaz zapisywania danych osobowe w ogólnodostępnych usługach typu chmury danych, jak np. Google Drive, Dropbox, OneDrive.
- Należy unikać korzystania z ogólnodostępnych sieci i punktów dostępowych. Korzystając z takich sieci zabronione jest przesyłanie służbowych danych osobowych.
- Administrator, mając na względzie bezpieczeństwo danych może w dowolnym momencie zablokować zdalnie udostępnione urządzenie oraz usunąć, bez wcześniejszego powiadomienia, w sposób nieodwracalny wszystkie zawarte tam dane, w tym również prywatne dane (pliki) użytkownika zapisane w urządzeniu. Administrator, mając na względzie bezpieczeństwo danych może również zdalnie zlokalizować urządzenie.

ROZDZIAŁ V

Zasady postępowania względem osób których dane dotyczą oraz względem danych

§ 18

Zapewnienie przejrzystej komunikacji i realizacja obowiązków informacyjnych

- Informacje przekazywane osobom, których dane dotyczą, należy formułować w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
- Należy uprawdopodobnić, iż informacje są przekazywane osobie, której dane dotyczą. W razie wątpliwości należy zażądać dodatkowych informacji w celu zweryfikowania tożsamości osoby, która się kontaktuje w celu uzyskania informacji.
- Przekazując informacje osobie, której dane dotyczą należy zadbać o to by informacja ta obejmowała wyłącznie dane go dotyczące. Należy dołożyć starań, by informacja przekazywana jednej osobie nie zdradzała informacji o innych.
- Zbierając informacje bezpośrednio od osoby, której dane dotyczą należy spełnić obowiązek informacyjny w zakresie i na warunkach wskazanych w art. 13 RODO.
- Zbierając informacje z innego źródła niż od osoby, której dane dotyczą należy spełnić obowiązek informacyjny w zakresie i na warunkach wskazanych w art. 14 RODO.
- Dopuszcza się realizację obowiązku informacyjnego na tzw. zasadzie „kaskadowej", polegającej na tym, że przekaz treści jest stopniowany, ograniczony i kolejno rozszerzany.
- Szczegółowe zasady dot. realizacji obowiązku informacyjnego uregulowano odrębnym dokumentem, tj. Zarządzeniem Burmistrza Radlina nr S.0050.0096.2018 z dnia 22 maja 2018 r. w sprawie wprowadzenia zasad dot. obowiązku informacyjnego w zakresie przetwarzania danych osobowych (wraz z ewentualnymi późniejszymi zmianami).

§ 19
Realizacja żądań osób, których dane dotyczą

Osobom, których dane są przetwarzane przysługują pełnie prawa przewidziane przepisami na ogólnych warunkach, bez uszczegółowienia tych zasad w Polityce.

§ 20
Zgody na przetwarzanie danych osobowych

Jeżeli podstawą przetwarzania danych osobowych jest zgoda osoby, której dane dotyczą, to przyzwolenie na przetwarzanie danych powinno być dobrowolne, konkretne, świadome i jednoznaczne. Na pracowniku merytorycznym prowadzącym sprawę ciąży obowiązek odebrania zgody na przetwarzanie danych osobowych od osoby której dane dotyczą, na nim

ciąży również obowiązek zachowania zasady rozliczalności, tj. stosownego udokumentowania faktu wyrażenia zgody. W niektórych przypadkach, udokumentowanie faktu wyrażenia zgody na przetwarzanie danych, przez osobę której dane dotyczą, może polegać na odnotowaniu tego faktu przez pracownika odbierającego zgodę (np. wyrażenie zgody podczas rozmowy telefonicznej). Odebranie zgody w takim przypadku pracownik potwierdza poprzez sporządzenie stosownej notatki.

§ 21
Udostępnianie danych osobowych

Jeśli zgodnie z przepisami prawa Administrator jest zobowiązany do udostępnienia danych osobowych wskazanym podmiotom, to upoważnieni pracownicy realizują ten wymóg zgodnie z zakresem swoich obowiązków służbowych stosując się ściśle do właściwych przepisów. Udostępnienia danych pracownik stosownie odnotowuje.

§ 22
Przekazywanie danych do państw trzecich lub organizacji międzynarodowych

Przekazywanie danych osobowych do państw trzecich oraz organizacji międzynarodowych każdorazowo wymaga przeprowadzenia przez pracownika analizy sprawy i przedłożenia jej Administratorowi, który na jej podstawie podejmie decyzję dot. ewentualnego przekazania danych osobowych.

§ 23
Powierzenia przetwarzania danych

- Jeśli wymagają tego okoliczności Administrator może podjąć decyzję o powierzeniu przetwarzania danych osobowych podmiotowi przetwarzającemu.
- Powierzenie danych osobowych podmiotowi przetwarzającemu następuje na podstawie pisemnej umowy.

- Wybierając podmiot przetwarzający dokłada się staranności, by podmiot przetwarzający zapewniał wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi bezpieczeństwa.
- Za wybór podmiotu przetwarzającego i sporządzenie umowy odpowiedzialny jest kierujący komórką organizacyjną prowadzącą sprawę (zlecający lub nadzorujący zadanie) lub pracownik merytoryczny jeżeli sprawę prowadzi jednoosobowo.
- Kierujący komórką organizacyjną prowadzącą sprawę lub pracownik merytoryczny, jeżeli sprawę prowadzi jednoosobowo, lub Administrator może przekazać projekt umowy do zaopiniowania Inspektorowi Ochrony Danych Osobowych.
- Po zatwierdzeniu umowy kierujący komórką organizacyjną prowadzącą sprawę lub pracownik merytoryczny, jeżeli sprawę prowadzi jednoosobowo, odnotowuje sporządzenie dokumentu w wewnętrznym serwisie udostępnionym pod adresem https://radlin.type.pl/udostepnienie .
- Na podstawie odnotowań sporządzonych w ww. serwisie, prowadzi się rejestr zawartych umów powierzenia przetwarzania danych osobowych.

§ 24

Współadministrowanie

Jeżeli Administrator wspólnie z innymi podmiotami ustala cele i sposoby przetwarzania danych osobowych, są oni współadministratorami. W drodze wspólnych uzgodnień współadministratorzy określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków. Projekt uzgodnień dot. współadministrowania danymi osobowymi, przed zatwierdzeniem przez Administratora opiniuje Inspektor Ochrony Danych. Zakres współpracy może być określony,w ten sposób, że szczegóły określa się w Rejestrach Czynności Przetwarzania poszczególnych współadministratorów.

ROZDZIAŁ VI

Działania nadzorcze, postępowania sprawdzające

§ 25

Nadzór nad ochroną danych

W celu zapewnienia ochrony wolności i praw osób, których dane dotyczą, a zwłaszcza bezpieczeństwa dotyczących ich danych osobowych, realizuje się w szczególności następujące zadania:

- prowadzi się Rejestr Czynności Przetwarzania i Rejestr Kategorii Czynności Przetwarzania,
- przeprowadza się ocenę ryzyka w zakresie naruszenia ochrony danych osobowych,
- jeśli to wymagane przeprowadza się ocenę skutków dla ochrony danych,
- jeśli to wymagane prowadzi się uprzednie konsultacje z organem nadzorczym,
- czuwa się nad aktualnością dokumentacji z zakresu ochrony danych osobowych,
- czuwa się nad przestrzeganiem zasad określonych w dokumentacji ochrony danych osobowych,
- czuwa się nad zgodnością przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
- prowadzi się postępowanie wyjaśniające w przypadku stwierdzenia naruszenia lub podejrzenia naruszenia ochrony danych osobowych,
- przeprowadza się okresowe podstępowania sprawdzające, kontrole lub audyty wewnętrzne.

§ 26
Rejestr Czynności Przetwarzania i Rejestr Kategorii Czynności Przetwarzania

Podmiot prowadzi Rejestr Czynności Przetwarzania (wykaz kategorii czynności przetwarzania)
i Rejestr Kategorii Czynności Przetwarzania. Szczegółowe zasady dot. ich sporządzania uregulowano odrębnym dokumentem, tj. Zarządzeniem Burmistrza Radlina nr S.0050.0087.2018
z dnia 11 maja 2018 r. w sprawie wprowadzenia procedury zarządzania ryzykiem w zakresie ochrony danych osobowych w Mieście Radlin (wraz z ewentualnymi późniejszymi zmianami).

§ 27
Ocena ryzyka, ocena skutków przetwarzania dla ochrony danych

Prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, określa się przez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych. Ryzyko szacuje się na podstawie obiektywnej i rzeczowej analizy, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko. Zasady identyfikacji ryzyk, szacowania ryzyk (ocena ryzyk), postępowania z ryzykami i ich monitorowania, itd., uregulowano odrębnym dokumentem, tj. Zarządzeniem Burmistrza Radlina nr S.0050.0087.2018 z dnia 11 maja 2018 r. w sprawie wprowadzenia procedury zarządzania ryzykiem w zakresie ochrony danych osobowych w Mieście Radlin (wraz z ewentualnymi późniejszymi zmianami).

§ 28

Postępowania sprawdzające, kontrole, audyty wewnętrzne

- W celu zapewnienia przestrzegania przepisów o ochronie danych osobowych Inspektor Ochrony Danych przeprowadza postępowania sprawdzające (nazywane zamiennie również kontrolami lub audytami wewnętrznymi). Działania te mogą w szczególności obejmować:
- sprawdzenie prawidłowości i aktualności dokumentacji z zakresu ochrony danych osobowych,
- sprawdzenie przestrzegania zasad i procedur określonych w dokumentacji ochrony danych osobowych,
- sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
- Postępowania sprawdzające przeprowadzane są okresowo.
- Inspektor Ochrony Danych nie musi informować Administratora o zamiarze prowadzenia postępowań sprawdzających oraz o fakcie prowadzenia postępowań. Inspektor Ochrony Danych informuje Administratora o wynikach prowadzonych postępowań sprawdzających.
- Inspektor Ochrony Danych nie musi powiadamiać osób poddawanych sprawdzeniu o zamiarze prowadzenia postępowań sprawdzających, fakcie prowadzenia postępowań i wynikach.
- Inspektor Ochrony Danych przygotowuje i gromadzi dokumentację przeprowadzonych postępowań sprawdzających.

ROZDZIAŁ VII
Naruszenia ochrony danych osobowych

§ 29
Postępowanie w przypadku stwierdzenia lub podejrzenia stwierdzenia naruszenia ochrony danych osobowych

- Za naruszenie ochrony danych uznaje się zdarzenia spełniające łącznie następujące przesłanki:
- naruszenie musi dotyczyć danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez podmiot, którego dotyczy naruszenie,
- skutkiem naruszenia musi być zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych,
- naruszenie jest skutkiem złamania zasad bezpieczeństwa danych.
- Wyróżnić można trzy typy zagrożeń:
- naruszenie poufności – polega na ujawnieniu danych osobowych nieuprawnionej osobie,
- naruszenie dostępności – polega na trwałej utracie lub zniszczeniu danych osobowych,
- naruszenie integralności – polega na zmianie treści danych osobowych w sposób nieautoryzowany.
- W proces wykrywania i obsługi naruszeń zaangażowani są: pracownicy merytoryczni zaangażowani w sprawę, Koordynator Techniczny (jeżeli naruszenie ma związek z elektronicznym przetwarzaniem danych), Inspektor Ochrony Danych, Administrator. W przypadku podejrzenia, że doszło do naruszenia, pracownik ujawniający natychmiast informuje Administratora lub Inspektora Ochrony Danych lub Koordynatora Technicznego (jeżeli naruszenie ma związek z elektronicznym przetwarzaniem danych).
- Każde z naruszeń ochrony danych osobowych (rozumiane jako 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) klasyfikuje się, czyli określa poziom wystąpienia ryzyka naruszenia praw i wolności osób fizycznych. Ryzyko naruszenia praw i wolności osób fizycznych jest obecne,

kiedy naruszenie może skutkować fizyczną, materialną lub niematerialną szkodą dla osób fizycznych, których dane naruszono. Szkodami takimi są np. dyskryminacja, kradzież tożsamości lub oszustwo dotyczące tożsamości, nadużycia finansowe, straty finansowe, nieuprawnione cofnięcie pseudonimizacji, utrata poufności danych osobowych chronionych tajemnicą zawodową, naruszenie dobrego imienia lub inne znaczące skutki gospodarcze lub społeczne dla danej osoby fizycznej, kiedy osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi. Jeżeli naruszenie dotyczy danych osobowych ujawniających pochodzenie etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych lub danych genetycznych, dotyczących zdrowia lub życia seksualnego, dane dotyczące seksualności, wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa, należy uznać, iż występuje duże prawdopodobieństwo takiej szkody. Duże prawdopodobieństwo takiej szkody może wystąpić również w innych przypadkach (np. zależenie od skali, indywidualnych przesłanek, kontekstu). Administrator określa wartość ryzyka naruszenia praw i wolności osób fizycznych jakie niesie za sobą naruszenie ochrony danych osobowych. Klasyfikując ryzyko należy mieć na uwadze procedurę zarządzania ryzykiem w zakresie ochrony danych osobowych w Mieście Radlin określoną Zarządzeniem nr S.0050.0087.2018 Burmistrza Radlina z dnia 11 maja 2018 roku (wraz z ewentualnymi późniejszymi zmianami).
Nie jest konieczne, aby ryzyko zmaterializowało się i by faktycznie doszło do naruszenia praw lub wolności. Zatem nie ma znaczenia, czy ostatecznie ich naruszenie nastąpi. Wystarczający jest fakt samego pojawienia się ryzyka naruszenia praw lub wolności.

- W zależności, z jakim poziomem ryzyka naruszenia praw i wolności osób fizycznych mamy do czynienia, inaczej kształtują się obowiązki w stosunku do organu nadzorczego, a także osób, których dane dotyczą.
- jeżeli naruszenie ochrony danych osobowych nie skutkuje naruszeniem praw lub wolności osób fizycznych - naruszenie należy wpisać do wewnętrznej ewidencji naruszeń, bez powiadamiania o nim organu nadzorczego i osoby, której dane dotyczą,
- jeżeli naruszenie ochrony danych osobowych może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych - naruszenie należy wpisać do wewnętrznej ewidencji naruszeń, powiadomić organ nadzorczy, bez powiadamiania osoby, której dane dotyczą,

- jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych - naruszenie należy wpisać do wewnętrznej ewidencji naruszeń, powiadomić organ nadzorczy oraz osoby, których dane dotyczą.
- W przypadku konieczności zawiadomienia o naruszeniu osób, których ono dotyczy należy przestrzegać następujących zasad:
- powinno być ono sporządzone w formie, która umożliwi tym osobom wielokrotne zapoznać się z jego treścią,
- zawiadomienie powinno zostać dostarczone do adresata w możliwie najkrótszym czasie, zasadniczo za pomocą środków komunikacji elektronicznej aby nie spowodować nieuzasadnionej zwłoki w przekazaniu informacji,
- Administrator bezpośrednio powiadamia osoby, których dane naruszono chyba, że wymagałoby to niewspółmiernie dużego wysiłku, w takim przypadku wydaje się publiczny komunikat lub stosuje podobny środek, aby w równie skuteczny sposób poinformować osoby, których dane dotyczą,
- zawiadomienie powinno zawierać co najmniej - dane kontaktowe Inspektora Ochrony Danych, opis możliwych konsekwencji naruszenia ochrony danych osobowych, opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu.
- Podmiot prowadzi wewnętrzną dokumentację naruszeń ochrony danych w formie stosownego rejestru. W rejestrze umieszcza się informacje o naruszeniu obejmujące okoliczności i przebieg naruszenia ochrony danych osobowych, naruszone dane osobowe, skutki i konsekwencje naruszenia oraz działania naprawcze. Rejestr prowadzony jest przy użyciu wewnętrznego serwisu udostępnionego pod adresem https://radlin.type.pl/naruszenie .
- W przypadku podjęcia decyzji o niezgłoszeniu naruszenia, wskazane jest udokumentowanie takiego faktu w ewidencji wraz z podaniem przyczyny, dla której uznaje się ryzyko naruszenia praw i wolności osób fizycznych za mało prawdopodobne.
- Podobnie jak w przypadku każdego incydentu związanego z bezpieczeństwem, ustala się, czy naruszenie było wynikiem błędu ludzkiego lub problemu systemowego i zbadać w jaki sposób można zapobiec powtórce incydentu - czy to poprzez lepsze procesy, dalsze szkolenia lub inne kroki naprawcze. Niezależnie od poziomu ryzyka, wprowadza się środki zaradcze mające na celu zminimalizowanie ryzyka i zabezpieczenia danych osobowych.

ROZDZIAŁ VIII

Przetwarzanie danych w systemach informatycznych

§ 30

Przedmiot i cele rozdziału

Niniejszy rozdział określa sposób zarządzania systemami informatycznymi, wykorzystywanymi
do przetwarzania informacji, w tym również danych osobowych w Podmiocie. Jego celem jest określenie zasad zabezpieczenia informacji i danych osobowych przed zagrożeniami, w tym zapewnienie takiego stopnia bezpieczeństwa danych osobowych, który odpowiadałby ryzyku, w rozumieniu art. 32 RODO. Rozdział opisuje m.in. sposoby nadawania uprawnień użytkownikom, określa sposób pracy w systemach informatycznych, procedury zarządzania oraz czynności mające wpływ na zapewnienie bezpieczeństwa systemów informatycznych Podmiotu.

§ 31

Nadawanie uprawnień

- Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba, która wcześniej otrzymała w wymaganym zakresie pisemne upoważnienie do przetwarzania danych osobowych.
- Nadanie uprawnień w systemach informatycznych dokonuje lub zleca Koordynator Techniczny na wniosek Administratora lub przełożonego użytkownika, po wcześniejszym zweryfikowaniu, czy osoba została stosowanie upoważniona do przetwarzania danych osobowych.
- Koordynator Techniczny prowadzi ewidencję użytkowników systemów informatycznych, w której odnotowuje również zakres nadanych uprawnień.

§ 32
Zmiana i blokowanie uprawnień

- Zmiany i blokowanie uprawnień użytkownika w systemach informatycznych dokonuje lub zleca Koordynator Techniczny, na wniosek przełożonego użytkownika lub Administratora.
- Przełożony użytkownika jest zobowiązany wnioskować o zmianę lub blokowanie uprawnień zawsze w przypadku zmiany zakresu obowiązków lub zmiany zakresu upoważnienia do przetwarzania danych osobowych użytkownika oraz zawsze w przypadku rozwiązania lub wygaśnięcia stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik.
- Koordynator Techniczny w prowadzonej ewidencji użytkowników systemów informatycznych, odnotowuje informacje dot. zmiany i blokowania uprawnień użytkownika.

§ 33
Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

- Dostęp do systemów informatycznych, w których przetwarzane są dane osobowe może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
- Identyfikator:
- jest w sposób jednoznaczny przypisany użytkownikowi, który jest odpowiedzialny za wszystkie czynności wykonane przy jego użyciu,
- nie powinien być zmieniany bez wyraźnej przyczyny i nie może być przydzielany innej osobie po wyrejestrowaniu użytkownika z systemu informatycznego.
- Hasło:
- musi składać się z zestawu co najmniej 8 znaków,
- musi zawierać małe i duże litery oraz cyfry lub znaki specjalne,
- nie może być identyczne z identyfikatorem ani imieniem lub nazwiskiem użytkownika,
- nie powinno składać się z kombinacji znaków mogących ułatwić jego odgadnięcie.
- Hasło przydzielone użytkownikowi po raz pierwszy musi być zmienione przez użytkownika po pierwszym udanym zalogowaniu się do systemu informatycznego.

•Hasło powinno być zmieniane przez użytkownika nie rzadziej niż co 30 dni. System informatyczny, jeżeli to możliwe, wymusza zmianę hasła po upływie 30 dni od dnia ostatniej zmiany hasła.

•Koordynator Techniczny może, w uzasadnionych sytuacjach, polecić dokonanie zmiany hasła przez użytkownika.

•Użytkownik zobowiązany jest w szczególności do:

•nieujawniania hasła innym osobom, w tym innym pracownikom, również po jego wygaśnięciu,

•przestrzegania zasad dotyczących jakości i częstości zmian hasła,

•wprowadzania hasła do systemu w sposób minimalizujący podejrzenie go przez inne osoby.

•W sytuacji, w której użytkownik zapomniał hasła, powinien on zwrócić się do Koordynatora Technicznego, który nadaje nowe hasło lub zleca jego nadanie.

•W przypadku podejrzenia zapoznania się z hasłem przez osobę nieuprawnioną użytkownik jest zobowiązany do natychmiastowej zmiany hasła.

•Ze względu na konieczność utrzymania ciągłości działania kluczowych systemów informatycznych nazwy i hasła kont administracyjnych do tych systemów powinny być przechowywane w formie pisemnej na papierze, w bezpiecznej lokalizacji, do której dostęp mają wyłącznie uprawnione osoby. Za zabezpieczenie ww. danych, ich aktualność oraz zaznajomienie kluczowych osób w Podmiocie z procedurą awaryjnego użycia danych odpowiada Koordynator Techniczny. W przypadku konieczności awaryjnego użycia nazw i haseł konieczne jest sporządzenie notatki służbowej ilustrującej zaistniałą sytuację. Notatka powinna zawierać co najmniej:

•imię i nazwisko oraz stanowisko osoby udostępniającej nazwę użytkownika i hasło,

•imię i nazwisko oraz stanowisko osoby pobierającej nazwę użytkownika i hasło,

•krótki opis sytuacji, która zmusiła do awaryjnego wykorzystania hasła.

§ 34

Procedura rozpoczęcia, zawieszenia i zakończenia pracy przeznaczona dla użytkowników stacjonarnych stacji roboczych

•Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym oraz w trakcie pracy każda osoba zobowiązana jest do zwrócenia szczególnej uwagi, czy nie wystąpiły symptomy mogące świadczyć o naruszeniu danych osobowych.

•Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.

•Jeżeli jest to możliwe, po przekroczeniu określonej dla wybranego systemu liczby prób logowania, system blokuje dostęp do zbioru danych na poziomie danego użytkownika. Odblokowania konta użytkownika dokonuje lub zleca Koordynator Techniczny.

•Jeżeli jest to możliwe, w przypadku bezczynności użytkownika trwającej więcej niż 10 minut dostęp do stacji roboczej blokowany jest automatycznie. Wznowienie pracy wymaga ponownego podania hasła użytkownika.

•Zmianę użytkownika na stacji roboczej każdorazowo musi poprzedzać wylogowanie się lub zablokowanie poprzedniego użytkownika. Niedopuszczalne jest aby dwóch lub większa ilość użytkowników wykorzystywała wspólnie jedno konto użytkownika.

•W przypadku czasowego opuszczenia stanowiska użytkownik zobowiązany jest zablokować stację roboczą (kombinacja klawiszy Windows+L) lub wylogować się z aplikacji i systemu na stacji roboczej, na której pracuje oraz sprawdzić czy nie zostały pozostawione bez nadzoru nośniki informacji zawierające dane osobowe. Wznowienie pracy w systemie operacyjnym oraz systemach przetwarzających dane może nastąpić jedynie po ponownym podaniu hasła użytkownika.

•Zakończenie pracy w systemie informatycznym dokonuje się poprzez wylogowanie użytkownika ze wszystkich aplikacji oraz zamknięcie systemu operacyjnego komputera i odczekanie do wyłączenia komputera.

•Niedopuszczalne jest fizyczne wyłączenie komputera przed zamknięciem uruchomionych aplikacji.

•Zabronione jest pozostawianie uruchomionego komputera, po zakończeniu dnia pracy.

§ 35

Procedura rozpoczęcia, zawieszenia i zakończenia pracy przeznaczona dla użytkowników komputerów przenośnych, tabletów i telefonów

•O ile to możliwe, przy przetwarzaniu danych osobowych na komputerach przenośnych obowiązuje procedura przeznaczona dla użytkowników stacjonarnych stacji roboczych.

•Użytkownicy, którym zostały powierzone komputery przenośne, tablety i telefony, powinni chronić je przed uszkodzeniem, kradzieżą i dostępem osób postronnych. Szczególną ostrożność należy zachować podczas ich transportu.

•Obowiązuje zakaz używania komputerów przenośnych, tabletów, telefonów przez osoby inne niż użytkownicy, którym zostały one powierzone, w tym przez domowników i osoby bliskie użytkownikowi.

•Praca na komputerze przenośnym, tablecie, telefonie możliwa jest po wprowadzeniu identyfikatora i hasła użytkownika lub przy użyciu innej formy bezpiecznej autoryzacji.

•Po zakończeniu pracy komputer przenośny, tablet, telefon należy blokować.

•W przypadku zauważenia symptomów mogących świadczyć o naruszeniu danych osobowych oraz w przypadku utraty urządzenia należy natychmiast poinformować Koordynatora Technicznego.

§ 36
Tworzenie kopii zapasowych zbiorów danych oraz oprogramowania służącego do ich przetwarzania

•Dane w systemach informatycznych podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych. Za proces tworzenia kopii zapasowych odpowiada Koordynator Techniczny, który je wykonuje lub zleca wykonanie.

•W systemach informatycznych wykorzystujących technologię klient-serwer kopie zapasowe wykonywane są po stronie serwera.

•Kopie zapasowe tworzone według następującego schematu:

•kopie zapasowe baz danych systemów informatycznych przetwarzających dane osobowe tworzone są automatycznie, **nie rzadziej niż co 24 godziny (od poniedziałku do piątku) oraz ręcznie każdorazowo przed aktualizacją danego systemu dziedzinowego,**

•kopie zapasowe oprogramowania systemowego serwerów (systemów fizycznych oraz systemów wirtualnych) oraz kopie zapasowe plików konfiguracyjnych aktywnych urządzeń sieciowych, tworzone są automatycznie lub ręcznie **nie rzadziej niż co 6 miesięcy,**

•kopie zapasowe oprogramowania systemowego stacji roboczych tworzone są ręcznie **każdorazowo po zainstalowaniu i skonfigurowaniu systemu oraz każdorazowo po przeprowadzeniu znaczących rekonfiguracji,**

•kopie zapasowe danych przetwarzanych na odległość w tzw. chmurach danych, poza siedzibą Podmiotu, tworzone są na zasadach określonych odrębnie,

•kopie zapasowe plików roboczych użytkowników (dot. tylko wybranych lokalizacji plików) tworzone są automatycznie **nie rzadziej niż jeden raz w tygodniu.**

•Pracownicy są zobowiązani do samodzielnego tworzenia kopii zapasowych danych przetwarzanych przez nich lokalnie na stacji roboczej poprzez skopiowanie plików do innej lokalizacji (katalog na serwerze, katalog na drugim dysku lokalnym). Częstotliwość i lokalizację określa i wskazuje Koordynator Techniczny indywidualnie.

•**Nie rzadziej niż co 6 miesięcy** Koordynator Techniczny przeprowadza lub zleca przeprowadzenia wyrywkowej analizy poprawności wykonania i odczytu kopii.

•Kopie zapasowe po ustaniu ich użyteczności są kasowane.

§ 37
Przenośne nośniki danych

•Pliki zawierające dane osobowe oraz pliki kopii zapasowych powinny być zapisywane na przenośnych nośnikach danych jedynie w formie zaszyfrowanej i przez czas niezbędny do spełnienia celu, w jakim zostały one na nośniku zapisane.

•Przenośne nośniki danych transportowane i przechowywane powinny być w sposób minimalizujący ryzyko ich uszkodzenia lub zagubienia.

•W przypadku gdy przenośny nośnik danych nie jest dłużej potrzebny należy z niego usunąć dane w sposób bezpieczny (np. poprzez nadpisanie).

•Dopuszcza się powierzenie niszczenia nośników danych wyspecjalizowanym podmiotom zewnętrznym, pod warunkiem zawarcia umowy powierzenia przetwarzania danych osobowych, zagwarantowania poufności danych przez usługodawcę, udokumentowania faktu zniszczenia nośników protokołem.

§ 38
Zabezpieczenie przed działalnością szkodliwego oprogramowania

•System informatyczny jest zabezpieczony przed działaniem niebezpiecznego oprogramowania w szczególności poprzez:

- stosowanie odpowiedniej ochrony antywirusowej na serwerach oraz stacjach roboczych wykorzystywanych do przetwarzania danych osobowych,
- stosowanie zapory sieciowej,
- aktualizację oprogramowania (w tym w szczelności systemów operacyjnych),
- konfigurację oprogramowania minimalizującą ryzyko naruszenia bezpieczeństwa,
- autoryzację użytkowników przy zachowaniu odpowiedniego poziomu komplikacji haseł dostępu.
- Aktualizację oprogramowania nadzoruje Koordynator Techniczny.
- Zasady zabezpieczenia systemu informatycznego przez użytkowników:
- zabrania się uruchamiania jakiegokolwiek oprogramowania, które nie zostało zatwierdzone do użytku w Podmiocie,
- zabrania się samowolnego podłączania (uruchamiania) przenośnych nośników danych niewiadomego pochodzenia,
- zabrania się samowolnego podłączania jakichkolwiek urządzeń nie będących własnością Podmiotu do portów komputera, urządzeń i sieci komputerowej - w przypadku zaistniałej konieczności wykorzystania urządzenia pochodzącego od podmiotu zewnętrznego, pracownik ma obowiązek przekazać go Koordynatorowi Technicznemu do przeanalizowania pod kątem obecności zagrożeń,
- zabrania się pobierania, zapisywania oraz uruchamiania plików niewiadomego pochodzenia,
- zabrania się otwierania poczty elektronicznej, której tytuł lub zawartość nie sugeruje związku z pełnionymi obowiązkami służbowymi lub budzi obawy dot. pochodzenia - w przypadkach wątpliwych należy skonsultować się z Koordynatorem Technicznym,
- zabrania się podawania służbowego adresu poczty elektronicznej w celach prywatnych, np. rejestracji na portalach, forach internetowych, w mediach społecznościowych itp.,
- dozwolone jest odwiedzanie jedynie zaufanych, znanych i popularnych serwisów i stron internetowych; należy sprawdzać bezpieczeństwo połączenia na stronach służących do logowania,
- należy każdy nośnik danych oraz każdy pobrany plik przeskanować systemem antywirusowym przed jego uruchomieniem,
- zabronione jest ingerowanie w ustawienia konfiguracyjne systemów informatycznych.
- Użytkownicy systemu informatycznego zobowiązani są do:

•monitorowania stanu oprogramowania antywirusowego na stanowisku roboczym i bezzwłocznego informowania Koordynatora Technicznego o jakichkolwiek odstępstwach od normy,

•powiadomienia Koordynatora Technicznego w przypadku zauważenia objawów mogących wskazywać na obecność niebezpiecznego oprogramowania; do objawów powyższych można zaliczyć m.in. istotne spowolnienie działania systemu informatycznego, nietypowe działanie aplikacji, nietypowe komunikaty, utratę danych lub modyfikację danych,

•natychmiastowego powiadomienia Koordynatora Technicznego o zauważonych przypadkach wykrycia zagrożeń przez oprogramowanie antywirusowe (komunikaty wskazujące wystąpienie zagrożenia).

•Systemy informatyczne przetwarzające dane osobowe zabezpieczone są przed ich utratą w wyniku awarii zasilania lub zakłóceń w sieci zasilającej poprzez zasilacze awaryjne zabezpieczające stacje robocze, serwery oraz kluczowe urządzenia, pozwalające na bezpieczne zamkniecie aplikacji przetwarzających dane osobowe w sposób umożliwiający poprawne zapisanie przetwarzanych danych.

§ 39

Przegląd i konserwacja systemów oraz nośników informacji służących do przetwarzania danych

•Wszelkie prace związane z przeglądem i konserwacją systemu informatycznego służącego do przetwarzania danych osobowych muszą uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.

•Przeglądu i konserwacji systemu okresowo dokonuje lub zleca Koordynator Techniczny.

•Przegląd powinien obejmować również wyrywkową analizę logów systemowych.

§ 40

Naprawa urządzeń komputerowych z danymi osobowymi

- Prace serwisowe na terenie Podmiotu mogą być wykonywane wyłącznie przez pracowników własnych lub upoważnionych przedstawicieli wykonawców zewnętrznych (pod nadzorem pracowników Podmiotu).
- Prace serwisowe poza terenem Podmiotu mogą być wykonywane wyłącznie w przypadku przekazania sprzętu bez nośników zawierających dane osobowe. W przypadku braku możliwości usunięcia nośnika zawierającego dane osobowe naprawa powinna zostać wykonana pod nadzorem Koordynatora Technicznego lub innego upoważnionego pracownika podmiotu.
- Przekazanie sprzętu teleinformatycznego do naprawy oraz wykonanie prac serwisowych na sprzęcie powinno być dokumentowane. Dokumentacja przechowywana jest przez Koordynatora Technicznego.
- Urządzenia, dyski lub inne elektroniczne nośniki informacji zawierające dane osobowe przeznaczone do:
- likwidacji - pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
- przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie.

Dokumentacja w tym zakresie przechowywana jest przez Koordynatora Technicznego.

§ 41

Procedury instalacji i aktualizacji oprogramowania na stacjach roboczych

- Instalacji i aktualizacji oprogramowania na stacjach roboczych dokonuje lub zleca Koordynator Techniczny.
- Aktualizacja oprogramowania powinna być przeprowadzana zgodnie z zaleceniami producentów oraz opinią rynkową, co do bezpieczeństwa i stabilności nowych wersji.
- Dopuszcza się wyłącznie instalację legalnego, licencjonowanego oprogramowania.
- Zabrania się instalowania oprogramowania bez zgody Koordynatora Technicznego.
- Dodatkowe aplikacje na komputerze mogą być używane wyłącznie po ich stosownym zatwierdzeniu.

§ 42

Zasady korzystania z poczty elektronicznej

•Każdy załącznik (nawet jeżeli pochodzi od zaufanego nadawcy) należy przeskanować systemem antywirusowym przed jego otwarciem na stacji roboczej.

•Nie należy otwierać załączników i odnośników w podejrzanych wiadomościach e-mail.

•Nie należy odpowiadać na wiadomości zawierające spam.

•Należy zgłaszać wpływ podejrzanej wiadomości do skrzynki poczty elektronicznej Koordynatorowi Technicznemu.

§ 43

Zasady posługiwania się podpisem elektronicznym

•Pracownicy, którzy zostali uprawnieni do posługiwania się podpisem elektronicznym i uzyskali odpowiednie środki dostępu (karta kryptograficzna, PIN, hasło do unieważnienia certyfikatu) mają obowiązek zabezpieczenia ich w sposób uniemożliwiający korzystanie z nich przez inne osoby.

•Pracownik ma obowiązek natychmiastowego poinformowania Administratora w przypadku:

•kradzieży, zgubienia karty lub dokumentów zawierających PIN lub hasło do unieważnienia certyfikatu,

•zmiany danych zawartych w certyfikacie karty podpisu elektronicznego,

•podejrzenia, że osoba nieuprawiona weszła w posiadanie PIN-u lub hasła do unieważnienia certyfikatu.

•Administrator może w każdej chwili anulować uprawnienia pracownika do posługiwania się podpisem elektronicznym przez wystąpienie ze stosownym wnioskiem do właściwego organu certyfikacyjnego o unieważnienie certyfikatu przed upływem okresu jego ważności.

•Na żądanie Administratora, pracownik ma obowiązek zwrotu karty kryptograficznej. W chwili zwrotu w obecności pracownika karta zostaje zniszczona poprzez przecięcie chip-a.

•W przypadku śmierci pracownika uprawnionego do posługiwania się podpisem elektronicznym Administrator podmiotu wszczyna procedurę unieważniającą certyfikat kwalifikowany.

§ 44

Brakowanie dokumentów

W przypadku dokonania brakowania dokumentów tradycyjnych należy usunąć lub zabezpieczyć przed ich odczytaniem odpowiadające im zapisy w systemach informatycznych. Dokonanie brakowania dokumentów tradycyjnych powinno być skorelowane z brakowaniem zapisów z bazy danych systemu informatycznego, a także z bieżących i archiwalnych kopii bezpieczeństwa.
W procedurze bierze udział Koordynator Techniczny.

§ 45

Prace na odległość

- Prowadzenie prac serwisowych, przez osoby nie będące pracownikami Podmiotu w trybie zdalnym odbywać się może jedynie za zgodą Koordynatora Technicznego i po zawarciu stosownej umowy powierzenia przetwarzania danych oraz pod warunkiem stosowania odpowiednich zabezpieczeń. Koordynator Techniczny prowadzi rejestr prac wykonywanych w trybie zdalnym. Udostępnianie połączenia w trybie zdalnym może odbywać się jedynie w godzinach pracy Podmiotu i pod nadzorem.
- Telepraca polegająca na świadczeniu pracy przez pracowników Podmiotu spoza jego siedzibą jest dopuszczalna za wiedzą i zgodą Administratora, pod warunkiem stosowania zabezpieczeń systemów informatycznych wskazanych w Polityce. Koordynator Techniczny nadaje lub zleca nadanie uprawnień dot. telepracy poszczególnym użytkownikom, co odnotowuje w prowadzonej dokumentacji.

§ 46

Szyfrowanie danych

Dąży się do zabezpieczania danych poprzez szyfrowanie. Szyfrowanie jest obowiązkowe dla danych osobowych przesyłanych w sieci Internet. Komunikacja z systemami udostępnionymi
na zasadzie aplikacji WWW (ang. World Wide Web), komunikacja e-mail, transfer plików FTP (ang. File Transfer Protocol), itp., są realizowane z wykorzystaniem zabezpieczenia SSL (ang. Secure Socket Layer) lub innej adekwatnej metody. Jeżeli jest to możliwe, komunikacja zewnętrzna pomiędzy systemami informatycznymi prowadzona jest w tzw. formie wirtualnej sieć prywatnej VPN (ang. Virtual Private Network) lub innej adekwatnej metody. Niezależnie

wysyłając (lub zapisując na nośnikach przenośnych) pliki zawierające dane osobowe użytkownik zawsze rozważa ich dodatkowe zabezpieczenie hasłem (w przypadku zastosowania
tego zabezpieczenia, hasło należy dostarczyć odbiorcy danych innym kanałem komunikacji).

§ 47
Dokumentowanie

Dąży się do prowadzenia maksymalnej dokumentacji dot. stosowanych systemów informatycznych, w tym w szczególności instrukcji dla użytkowników systemów i instrukcji dla administratorów, dokumentacji opisującej przepływy danych pomiędzy poszczególnymi systemami (nie dotyczy znanych ogólnodostępnych mechanizmów wymiany danych np. ZUS Płatnik) i struktury zbiorów danych, danych kontaktowych na wypadek wystąpienia awarii. Dąży się do stosowania systemów tylko jednoznacznie dokumentujących działania użytkowników. Działania w tym zakresie nadzoruje Koordynator Techniczny.

§ 48
Postępowanie w przypadku naruszenia bezpieczeństwa

- Użytkownik zobowiązany jest zawiadomić Koordynatora Technicznego o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu informatycznego, a w szczególności o:
- naruszeniu identyfikatora lub hasła dostępu,
- częściowym lub całkowitym braku dostępu do danych,
- dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień,
- braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów serwera,
- wykryciu szkodliwego oprogramowania na stacji roboczej,
- zauważeniu elektronicznych śladów próby włamania do systemu informatycznego,
- znacznym spowolnieniu działania systemu informatycznego,
- podejrzeniu kradzieży sprzętu komputerowego,
- zmianie położenia sprzętu komputerowego,
- zauważeniu śladów usiłowania lub dokonania włamania.

•Do czasu przybycia na miejsce Koordynatora Technicznego należy:

•o ile istnieje taka możliwość, niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego zdarzenia, a następnie uwzględnić w działaniu również ustalenie jego przyczyn lub sprawców,

•rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,

•zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,

•zastosować się do instrukcji i regulaminów lub dokumentacji aplikacji, jeśli odnoszą się one do zaistniałego przypadku,

•nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia.

•Koordynator Techniczny po otrzymaniu zawiadomienia niezwłocznie:

•podejmuje czynności zmierzające do weryfikacji informacji zawartych w zawiadomieniu,

•gdy to właściwe podejmuje czynności zmierzające do minimalizacji ewentualnych negatywnych konsekwencji zaistniałego zdarzenia oraz chroniące system informatyczny przed ponownym naruszeniem,

•o ile to możliwe zabezpiecza dowody przydatne do ustalenia przyczyn, typu i skutków naruszenia,

•może zarządzić odłączenie części systemu informatycznego dotkniętej incydentem od pozostałej jego części,

•może zarządzić odtwarzanie danych z kopii zapasowych po uprzednim upewnieniu się, że odtwarzane dane zapisane zostały przed wystąpieniem incydentu,

•mając na uwadze § 29 Polityki, w przypadkach uzasadnionych, powiadamia Inspektora Ochrony Danych lub Administratora.

ROZDZIAŁ IX

Monitoring wizyjny

§ 49

Zasady funkcjonowania monitoringu wizyjnego

Miasto objęte jest monitoringiem wizyjnym obsługiwanym przez Straż Miejską w Radlinie (z siedzibą - ul. Mariacka 93, 44-310 Radlin) będąca komórka organizacyjną Urzędu Miasta Radlin. System monitoringu miejskiego może obejmować również otoczenie Podmiotu. Ponadto Administrator może stosować dodatkowy wewnętrzny system monitoringu wizyjnego (obejmujący obszar na zewnątrz i wewnątrz siedziby Podmiotu). Monitoring wizyjny działa wg następujących zasad:

- celem jego działania jest zapewnienie bezpieczeństwa mienia oraz osób,
- monitoring funkcjonuje całodobowo,
- system monitoringu wizyjnego składa się w szczególności z kamer rejestrujących zdarzenia w rozdzielczości umożliwiających identyfikację osób; urządzenia rejestrującego i zapisującego obraz na nośniku fizycznym; monitorów pozwalających na podgląd rejestrowanych zdarzeń,
- rejestracji podlega tylko obraz (wizja) z kamer systemu monitoringu,
- dostęp do zarejestrowanych treści możliwy jest wyłącznie dla osób uprawnionych, w tym upoważnionych pracowników Podmiotu, pracowników firmy świadczącej usługi obsługi technicznej systemu; funkcjonariuszy uprawnionych służb,
- dopuszcza się możliwość przetwarzana danych na odległość poza siedzibą Podmiotu, w tzw. chmurze danych,
- zapis monitoringu może być udostępniony jedynie uprawnionym organom w zakresie prowadzonych przez nie czynności prawnych, na ich wniosek; nie udostępnia się nagrań osobom fizycznym,
- udostępniający zapis monitoringu, ewidencjonuje udostępnienie w stosownym rejestrze,
- okres przechowywania danych monitoringu nie jest dłuższy, niż przewidziany przepisami; dane ulegają usunięciu poprzez nadpisanie danych na urządzeniu rejestrującym obraz,
- w uzasadnionych przypadkach na podstawie wniosków osób fizycznych lub uprawnionych organów, w szczególności, gdy urządzenia monitoringu wizyjnego zarejestrowały zdarzenie związane z naruszeniem bezpieczeństwa osób i mienia, okres przechowywania danych może ulec wydłużeniu o czas niezbędny do zakończenia postępowania, którego przedmiotem jest zdarzenie zarejestrowane przez monitoring wizyjny,
- dopuszcza się występowanie nieznacznych różnic między czasem rzeczywistym a czasem uwidocznionym na materiale z monitoringu, z uwagi na brak synchronizacji systemu z zewnętrznym źródłem czasu,

•system nie jest wyposażony w funkcje automatycznej identyfikacji osób i reagowania na incydenty,

•obszary objęte monitoringiem oznacza się w sposób widoczny i czytelny informacją o monitorowaniu; przy czym w zakresie monitoringu miejskiego obsługiwanego przez Straż Miejską w Radlinie jako oznaczenie objęcia monitoringiem obszaru całego miasta, uważa się umieszczenie tablic stosownych treści pod znakami drogowymi oznaczającymi wjazd do miejscowości.

ROZDZIAŁ X

Pozostałe ustalenia

§ 50

Ciągłość działania

Celem kontynuowania działalności Podmiotu w kluczowych procesach w przypadku wystąpienia zdarzeń niepożądanych, wdrożono opisane we wcześniejszych częściach niniejszej Polityki zabezpieczenia (poszczególne procedury w przypadku naruszenia konkretnych zasad bezpieczeństwa, zasady tworzenia kopii bezpieczeństwa, zasady dostępu do haseł administracyjnych, dokumentowania, itd.) oraz ustanowiono zastępstwa. W zakresie sprawy dotyczących ochrony danych osobowych kwestię zastępstw uregulowano odrębnym dokumentem, tj. Zarządzeniem Burmistrza Radlina nr S.0050.0205.2018 z dnia 06 listopada 2018 r. w sprawie wprowadzenia systemu szkoleń wewnętrznych dot. ochrony danych osobowych i wyznaczeniu koordynatorów ds. ochrony danych w jednostkach organizacyjnych Miasta Radlin (wraz z ewentualnymi późniejszymi zmianami).

§ 51

Dokumenty odrębne przywołane w Polityce

•Zarządzenie Burmistrza Radlina nr S.0050.0087.2018 z dnia 11 maja 2018 r. w sprawie wprowadzenia procedury zarządzania ryzykiem w zakresie ochrony danych osobowych w Mieście Radlin (§ 26, § 27, § 29 Polityki).

- Zarządzenie Burmistrza Radlina nr S.0050.0096.2018 z dnia 22 maja 2018 r. w sprawie wprowadzenia zasad dot. obowiązku informacyjnego w zakresie przetwarzania danych osobowych (§ 18 Polityki).
- Zarządzenie Burmistrza Radlina Nr S.0050.0205.2018 z dnia 06 listopada 2018 r. w sprawie wprowadzenia systemu szkoleń wewnętrznych dot. ochrony danych osobowych i wyznaczeniu koordynatorów ds. ochrony danych w jednostkach organizacyjnych Miasta Radlin (§ 6, § 8, § 50 Polityki).

§ 52

Postanowienia końcowe

- Polityka podlega okresowym przeglądom pod kątem aktualności i zakresu stosowania.
- W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie odpowiednie przepisy dotyczące ochrony danych osobowych, a w zakresie systemów informatycznych również instrukcje obsługi tych systemów i zalecenia producentów.
- Naruszenie zasad i procedur określonych w niniejszej Polityce może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych lub jako nienależyte wykonanie umowy w rozumieniu Kodeksu cywilnego.