POLITYKA BEZPIECZEŃSTWA
I OCHRONY PRZETWARZANIA DANYCH OSOBOWYCH
W XI LICEUM OGÓLNOKSZTAŁCĄCYM
W ŁODZI

Polityka bezpieczeństwa i ochrony danych osobowych obowiązująca w XI Liceum Ogólnokształcącym w Łodzi

Spis treści

Wprowadzenie 3
Rozdział I Przepisy wprowadzające 4
Rozdział II Podstawowe zasady związane z przetwarzaniem danych osobowych 7
Rozdział III Zarządzanie bezpieczeństwem danych osobowych 9
Rozdział IV Transfer danych osobowych 16
Rozdział V Opis zdarzeń naruszających ochronę danych osobowych 18
Rozdział VI System informatyczny i zabezpieczenie danych osobowych 20
Rozdział VII Kontrola przestrzegania zasad zabezpieczenia danych osobowych 27
Rozdział VIII Postępowanie w przypadku naruszenia ochrony danych osobowych 27
Rozdział IX Postanowienia końcowe 29
Spis załączników „Polityki bezpieczeństwa i ochrony danych osobowych”: 29

Wprowadzenie

Niniejszy dokument opisuje reguły oraz procedury dotyczące sposobu przetwarzania oraz bezpieczeństwa przetwarzania danych osobowych, w tym przetwarzania danych zużyciem systemów informatycznych, przez Administratora danych osobowych, tj. XI Liceum Ogólnokształcące w Łodzi, z siedzibą pod adresem: Łódź, ul. dr. Stefana Kopcińskiego 54, 90-032 Łódź. Dokument ma zastosowanie do przetwarzania wszelkich danych osobowych gromadzonych przez Administratora, pobieranych bezpośrednio od osób, których dane dotyczą, a także z innych źródeł:

a) pobieranych przez:
   - pracowników,
   - osoby trzecie, w tym rodziców i opiekunów prawnych,
   - za pośrednictwem stron internetowych
   - za pośrednictwem poczty elektronicznej, w tym przez adres e-mail placówki
b) danych osobowych, które Administrator danych osobowych przetwarza jako podmiot przetwarzający,
c) danych osobowych udostępnionych Administratorowi danych osobowych.

Opisane reguły i procedury określają granice dopuszczalnego zachowania wszystkich osób przetwarzających dane osobowe zatrudnionych oraz współpracujących z Administratorem danych osobowych. Dokument zwraca uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone granice, oraz procedury postępowania dla minimalizowania skutków zagrożeń i zapobiegania im w związku z naruszeniem bezpieczeństwa przetwarzania danych osobowych.

Polityka ochrony danych osobowych obowiązuje wszystkich pracowników (bez względu na to, czy podstawą zatrudnienia jest stosunek pracy, czy umowa cywilnoprawna) i współpracowników Administratora danych osobowych dokonujących jakichkolwiek operacji na danych osobowych. Realizacja postanowień tego dokumentu ma zapewnić ochronę danych osobowych, właściwą ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa przetwarzania oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemach informatycznych.

Polityka bezpieczeństwa została opracowana w oparciu o zasady wynikające rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, a także wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko” do celów rozporządzenia 2016/679, to jest Wytyczne Grupy Roboczej art. 29 przyjęte w dniu 4kwietnia 2017r. (z późniejszymi zmianami) oraz ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. poz. 1000).

Polityka ochrony danych osobowych określa przede wszystkim sposób postępowania w przypadku:

a) przetwarzania danych osobowych, niezależnie od tego, z jakich źródeł dane te pochodzą, w jakim celu są przetwarzane oraz jakich kategorii danych osobowych dotyczy przetwarzanie,

b) stwierdzenia naruszenia bezpieczeństwa ochrony danych osobowych,

c) stwierdzenia naruszenia zabezpieczenia systemów informatycznych, w jakich dane są przetwarzane,

d) zapobiegania skutkom naruszenia bezpieczeństwa przetwarzania danych osobowych.

Celem niniejszego dokumentu oraz opisanych w nim reguł i procedur jest – zwłaszcza w odniesieniu do pracowników, którzy w toku pracy przetwarzają dane osobowe lub mają z nimi styczność – spełnienie następujących postulatów:

a) spełnienie wymagań prawnych dotyczących przetwarzania danych osobowych jako cel podstawowy,

b) zwiększenie świadomości co do wagi i wartości informacji wynikających zdanych osobowych,

c) konieczność ochrony danych osobowych oraz dóbr osobistych osób, których dane dotyczą,

d) ochrona informacji oraz zapewnienie prywatności i godności każdego pracownika, ucznia oraz innych osób, których dane dotyczą,

e) ciągłe uczenie się i wyciąganie wniosków z błędów,

f) stałe doskonalenie rozwiązań dostosowujących działania do nowych celów oraz potencjalnych zagrożeń związanych z przetwarzaniem danych osobowych,

g) uświadomienie i zapewnienie, że wszyscy pracownicy są zobowiązani do przestrzegania szczegółowych zasad postępowania wskazanych w niniejszym dokumencie.

Rozdział I
Przepisy wprowadzające

1. Definicje

Użyte w niniejszym dokumencie określenia oznaczają:

a) **Administrator danych osobowych (Administrator)** – XI Liceum Ogólnokształcące w Łodzi, z siedzibą pod adresem: Łódź, ul. dr. Stefana Kopcińskiego 54, 90-032 Łódź.

b) **Administrator systemu** – osoba odpowiedzialna za zapewnienie ciągłości i poprawności działania systemu informatycznego,

c) **Użytkownik** – osoba upoważniona przez Administratora danych osobowych do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym, która posiada ustalony indywidualny identyfikator oraz hasło,

d) **zbiór danych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie,

e) **baza danych osobowych (baza)** – każdy posiadający strukturę zbiór danych, które są danymi osobowymi lub mogą stanowić dane osobowe, dostępny według określonych kryteriów,

f) **dane osobowe (dane)** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,

g) **hasło** – ciąg znaków literowych, cyfrowych lub innych, pozwalający na dostęp do systemu informatycznego, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,

h) **identyfikator** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do dostępu do systemu informatycznego,

i) **Inspektor ochrony danych (IOD)** – osoba wyznaczona przez Administratora w celu informowania i doradzania Administratorowi, podmiotowi przetwarzającemu, pracownikowi w zakresie obowiązków prawnych ochrony danych osobowych i niniejszej Polityki oraz w celu monitorowania i przestrzegania oraz działania jako punkt kontaktowy dla osób, których dane są przetwarzane i organu nadzorczego,

j) **integralność** – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

k) **Podmiot przetwarzający** – podmiot, o którym mowa wart. 28 RODO, który dokonuje czynności przetwarzania danych osobowych na zlecenie Administratora danych osobowych,

l) **Polityka** – niniejsza Polityka bezpieczeństwa i ochrony danych osobowych obowiązująca u Administratora,

m) **poufność** – właściwość zapewniająca, że dane osobowe nie są udostępniane nieupoważnionym podmiotom,

n) **profilowanie** – dowolne zautomatyzowane przetwarzanie danych osobowych pozwalające ocenić czynniki osobowe osoby fizycznej, a w szczególności analizować lub prognozować aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą – o ile wywołuje skutki prawne względem tej osoby lub w podobny sposób znacząco na nią wpływa,

o) **przetwarzanie danych osobowych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie i inne, a zwłaszcza te, które wykonuje się w systemach informatycznych,

p) **anonimizacja/ 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; anonimizacja – w przeciwieństwie do pseudonimizacji – jest procesem nieodwracalnym,

q) **PUODO** – Prezes Urzędu Ochrony Danych Osobowych pełniący funkcję organu nadzorczego na terenie Rzeczypospolitej Polskiej w rozumieniu art.4 pkt. 21 w zw. zart.51 ust.1 RODO,

r) **RODO** – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27kwietnia 2016r. 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),

s) **sieć telekomunikacyjna** – sieć telekomunikacyjna oraz publiczna sieć telekomunikacyjna w rozumieniu odpowiednio art.2 pkt. 35 oraz art.2 pkt. 29 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. z 2017 r. poz.1907 ze zm.), w tym w szczególności Internet,

t) **system informatyczny** – zbiór powiązanych ze sobą elementów: serwerów z systemami operacyjnymi, systemu zarządzania bazami danych osobowych, oprogramowania (programów użytkowych), urządzeń końcowych (komputerów, drukarek) oraz urządzeń służących do komunikacji między sprzętowymi elementami systemu,

u) **Ustawa** – Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. poz.1000).

2. Podstawa prawna

1. Polityka jest zgodna z następującymi aktami prawnymi:

   a) Konstytucją Rzeczypospolitej Polskiej,

   b) RODO,

   c) Ustawą,

   d) przepisami innych aktów prawnych powszechnie obowiązujących w zakresie, w jakim dotyczą ochrony danych osobowych.

Rozdział II
Podstawowe zasady związane z przetwarzaniem danych osobowych

1. Zakres obowiązywania

1.1. Ochrona danych osobowych przetwarzanych przez Administratora danych osobowych obowiązuje wszystkie osoby, które mają dostęp do danych osobowych podlegających przetwarzaniu, bez względu na zajmowane stanowisko oraz miejsce wykonywania, jak również charakter łączącej je umowy lub stosunku pracy z Administratorem danych osobowych.

1.2. Pracownicy oraz współpracownicy Administratora danych osobowych są zobligowani do stosowania niezbędnych środków zapobiegających ujawnieniu danych osobowych osobom nieupoważnionym, w tym w szczególności procedur i reguł wskazanych w niniejszej Polityce.

1.3. Zachowanie tajemnicy w zakresie danych osobowych obowiązuje zarówno podczas trwania stosunku pracy lub innej umowy łączącej Użytkownika z Administratorem danych osobowych, jak również po ustaniu stosunku pracy lub innej umowy.

1.4. Inspektor ochrony danych osobowych jest odpowiedzialny za nadzór nad tworzeniem, wdrażaniem, administracją i interpretacją niniejszej Polityki oraz innych standardów, zaleceń oraz procedur dotyczących ochrony danych osobowych obowiązujących u Administratora danych osobowych.

1.5. Polecenia Inspektora ochrony danych osobowych, a także innych osób delegowanych i wyznaczonych do działań związanych danych osobowych oraz w zakresie ochrony informacji i bezpieczeństwa systemu informatycznego muszą być bezwzględnie wykonywane przez Administratora danych osobowych, wszystkich jego pracowników, współpracowników i użytkowników systemu informatycznego, którzy zajmują się przetwarzaniem danych osobowych.

1.6. Wszędzie, gdzie jest mowa o pracownikach, należy przez to rozumieć zarówno osoby zatrudnione w ramach stosunku pracy, jak również w oparciu o umowę cywilnoprawną (w tym umowę-zlecenie oraz umowę o współpracy i o świadczenie usług).

2. Zasady przetwarzania oraz ochrony danych osobowych

2.1. Przetwarzanie danych osobowych przez Administratora danych osobowych może odbywać się tylko zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą.

2.2. Dane osobowe zbierane są przez Administratora danych osobowych jedynie w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.

2.3. Dane osobowe mogą być przetwarzane przez Administratora danych osobowych w sposób adekwatny, stosowny oraz ograniczony do tego, co niezbędne, do celów, w których są przetwarzane.

2.4. Administrator danych osobowych zobowiązany jest do przetwarzania danych prawidłowych i w razie potrzeby, szczególnie na wniosek osoby, której dane dotyczą, ich uaktualniania.

2.5. Dane osobowe są przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.

2.6. Dane osobowe są przetwarzane w sposób zapewniający odpowiednie ich bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

2.7. Przetwarzanie danych osobowych może odbywać się wyłącznie w obszarach do tego celu przeznaczonych. Obszary przetwarzania i wykaz środków technicznych, w których dopuszczalne jest przetwarzanie danych osobowych, stanowi Załącznik nr 1 do niniejszej Polityki.

2.8. W szczególnych przypadkach możliwe jest przetwarzanie danych osobowych poza wyznaczonym obszarem (np. na komputerach przenośnych), jednak wymaga to poinformowania oraz zgody Administratora danych osobowych.

2.9. Dostęp do pomieszczeń, w których są przetwarzane dane osobowe, oraz do pomieszczeń, w których znajdują się serwery baz danych osobowych lub przechowywane są kopie zapasowe, mogą mieć wyłącznie osoby, które posiadają do tego odpowiednie upoważnienie nadane przez Administratora danych osobowych.

2.10. Przetwarzania danych osobowych może dokonywać wyłącznie osoba posiadająca upoważnienie do ich przetwarzania, tj. osoba, która znajduje się w „Ewidencji osób upoważnionych do przetwarzania danych osobowych", stanowiącej Załącznik nr 6 do niniejszej Polityki, prowadzonej przez Administratora danych osobowych.

2.11. Wszystkie osoby przetwarzające dane osobowe z upoważnienia Administratora obowiązuje *zasada czystego biurka*, zabraniająca pozostawiania jakichkolwiek dokumentów z danymi osobowymi podczas nieobecności pracownika przy stanowisku pracy. Niedozwolone jest pozostawianie dokumentacji papierowej zdanymi osobowymi na stanowisku pracy po jej zakończeniu, gdyż należy uniemożliwić zapoznanie się zdanymi osobowymi osobom nieuprawnionym.

2.12. W przypadku opuszczenia stanowiska pracy osoba przetwarzająca dane osobowe powinna wylogować się z systemu lub zablokować dostęp do pulpitu stacji roboczej, z której korzysta przy przetwarzaniu danych osobowych. Ponadto w razie opuszczenia stanowiska pracy lub zakończenia pracy z systemem informatycznym należy zamykać pliki zawierające

dane osobowe. Uniemożliwi to dostęp do danych osobowych osobie nieupoważnionej (*polityka czystego ekranu*).

3. Podstawa prawna do przetwarzania danych osobowych

3.1. Przetwarzanie danych osobowych przez Administratora możliwe jest pod warunkiem, że:

a) osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub w 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,

d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej,

e) przetwarzanie 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 jej danych osobowych, w szczególności, gdy osoba, której dane dotyczą, jest dzieckiem.

3.2. Administrator danych osobowych zobowiązuje się nie przetwarzać danych osobowych, jeżeli nie spełni jednej z przesłanek, o których mowa w punkcie poprzedzającym.

Rozdział III
Zarządzanie bezpieczeństwem danych osobowych

1. Przetwarzanie danych osobowych

1.1. Administrator dokonuje przetwarzania danych osobowych w określonych zbiorach danych osobowych jako ich Administrator, a także – w określonych przypadkach – jako podmiot przetwarzający.

1.2. Wykaz zbiorów danych osobowych wraz z opisem ich struktury oraz rejestrem czynności przetwarzania danych osobowych zawiera Załącznik nr 2 do niniejszej Polityki.

1.3. W przypadku istnienia więcej niż jednego zbioru danych osobowych dla każdego zbioru prowadzony jest odpowiednio rejestr czynności przetwarzania, o którym mowa w punkcie poprzedzającym.

1.4. Załącznik, o którym mowa w rozdziale III pkt. 1.2., powinien być aktualizowany po wprowadzeniu istotnych zmian w strukturze danego zbioru danych osobowych, który

opisuje. W przypadku systemów, które są rozbudowywane, wprowadzone zmiany powinny zostać uwzględnione w niniejszej Polityce.

2. Obowiązek informacyjny

2.1. Każda osoba, której dane osobowe będą przetwarzane przez Administratora danych osobowych, ma prawo do bycia informowaną o przetwarzaniu danych osobowych.
W związku z tym, wobec osób, których dane dotyczą, a których dane osobowe są przez Administratora danych osobowych przetwarzane, Administrator zobowiązany jest wypełniać obowiązek informacyjny.

2.2. Obowiązek informacyjny spełniany jest wobec wszystkich osób, których dane dotyczą, a które to dane są przez Administratora przetwarzane, niezależnie od celu ich przetwarzania.

2.3. Obowiązek informacyjny Administratora powinien obejmować ujawnienie informacji takich, jak:

a) tożsamość i dane kontaktowe Administratora oraz – gdy ma to zastosowanie – tożsamość i dane kontaktowe przedstawiciela Administratora,

b) imię i nazwisko oraz dane kontaktowe Inspektora ochrony danych osobowych,

c) cele przetwarzania danych osobowych oraz podstawa prawna tego przetwarzania,

d) gdy ma to zastosowanie – prawnie uzasadnione interesy realizowane przez Administratora lub przez stronę trzecią,

e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,

f) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej,

g) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,

h) informacja oprawie do żądania od Administratora przez osobę, której dane dotyczą, dostępu do jej danych osobowych, ich sprostowania, usunięcia (*bycia zapomnianym*), ograniczenia przetwarzania, przenoszenia, wniesienia sprzeciwu wobec przetwarzania oraz do złożenia skargi do PUODO,

i) informacja oprawie do cofnięcia zgody udzielonej przez osobę, której dane dotyczą, w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,

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

k) informacja o zautomatyzowanym podejmowaniu decyzji, w tym oprofilowaniu oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania,

a także oznaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

2.4. Obowiązek informacyjny Administrator spełnia przez przekazanie informacji drogą elektroniczną lub przekazanie informacji w klauzulach informacyjnych, umowach zawieranych z osobami, których dane dotyczą.

2.5. Niedopuszczalne jest niewypełnienie obowiązku informacyjnego przez Administratora danych osobowych lub jego pracowników.

2.6. Ponadto, jeżeli Administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego (PUODO) oraz skorzystania ze środków ochrony prawnej przed sądem.

3. Ocena skutków przetwarzania danych osobowych

3.1. Administrator danych osobowych szacuje prawdopodobieństwo naruszenia bezpieczeństwa przetwarzania danych osobowych przez przeprowadzanie oceny skutków przetwarzania danych osobowych przed wprowadzeniem nowych rozwiązań, które mogą mieć wpływ na to przetwarzanie u Administratora.

3.2. Wykaz skutków przetwarzania danych osobowych dla ich bezpieczeństwa w poszczególnych bazach danych osobowych Administrator sporządza w przypadku wystąpienia procesu przetwarzania zobowiązującego do sporządzenia wykazu skutków.

3.3. W przypadku istnienia więcej niż jednej bazy, dla której należy przeprowadzić ocenę skutków przetwarzania danych osobowych, powinien zostać sporządzony odrębny załącznik do niniejszej Polityki dla każdej bazy z osobna.

3.4. Administrator przeprowadza ocenę skutków przetwarzania danych osobowych w przypadku jednoczesnego wystąpienia co najmniej dwóch z poniższych przypadków:

a) ocena iscoring, w tym profilowanie i przewidywanie, w szczególności dotyczące takich czynników osobowych osoby, której dane dotyczą, jak świadczenie pracy, sytuacja ekonomiczna, zdrowie, osobiste preferencje, zainteresowania, wiarygodność, zachowanie, lokalizacja czy poruszanie się,

b) zautomatyzowane podejmowanie decyzji, w tym profilowanie, wywołujące skutki prawne lub wpływające na osobę, której dane dotyczą, w podobny sposób,

c) systematyczne monitorowanie mające na celu obserwowanie, monitorowanie lub kontrolowanie osoby, której dane dotyczą, w tym systematyczne monitorowanie miejsc dostępnych publicznie,

d) przetwarzanie szczególnych kategorii danych osobowych zart.9 ust.1 (dane wrażliwe) i art.10 (dane dotyczące karalności) RODO,

e) przetwarzanie danych osobowych na dużą skalę,

f) przetwarzanie danych osobowych podlegających łączeniu lub dopasowywaniu,

g) wykorzystanie do przetwarzania danych osobowych innowacyjnych rozwiązań technicznych lub organizacyjnych, zwłaszcza w kontekście nowatorskich technologii, wykorzystujących np. biometrię,

h) transfer danych poza granice Europejskiego Obszaru Gospodarczego, a zwłaszcza do USA,

i) przetwarzanie danych, które samo w sobie utrudnia osobie, której dane dotyczą, wykonywanie przysługujących jej praw lub korzystanie z usługi czy zawarcie umowy.

3.5. Ocena skutków przetwarzania danych osobowych dokonana przez Administratora danych osobowych powinna zawierać co najmniej:

a) opis planowanych operacji przetwarzania danych osobowych i celów tego przetwarzania,

b) ocenę niezbędności i proporcjonalności przetwarzania w stosunku do celów, tj. wskazanie, czy określonego – potencjalnie ryzykownego – działania można uniknąć lub, jeśli nie ma takiej możliwości, jakie środki zastosowano, aby ryzyko zostało zminimalizowane,

c) ocenę ryzyka naruszenia praw i wolności osoby, której dane dotyczą, w szczególności, aby Administrator, jego pracownicy i współpracownicy zdawali sobie sprawę z ryzyka, jakie niesie wykorzystywana technologia,

d) środki planowane w celu zaradzenia ryzyku oraz wykazania zgodności operacji przetwarzania danych osobowych zobowiązującymi przepisami prawa.

4. Rejestr czynności przetwarzania danych osobowych/Rejestr kategorii czynności przetwarzania danych podmiotu przetwarzającego

4.1. Administrator danych osobowych prowadzi rejestr czynności przetwarzania danych osobowych w poszczególnych bazach danych osobowych.

4.2. Podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania danych Podmiotu przetwarzającego.

4.3. Rejestr czynności przetwarzania danych osobowych zawiera informacje dotyczące:

a) danych identyfikujących Administratora, w tym jego nazwy oraz danych kontaktowych,

b) celów, w jakich są przetwarzane dane osobowe,

c) opisu kategorii osób, których dane dotyczą, oraz kategorii danych osobowych,

d) kategorii odbiorców, którym dane zostały lub zostaną ujawnione,

e) odnotowania faktu przekazania danych osobowych do państwa trzeciego,

f) planowanych terminów usunięcia poszczególnych kategorii danych osobowych,

g) ogólnego opisu technicznego i organizacyjnego środków bezpieczeństwa.

4.4. Rejestr kategorii czynności przetwarzania danych podmiotu przetwarzającego zawiera informacje dotyczące:

a) danych identyfikujących Podmiot przetwarzający oraz Administratora, w imieniu którego działa Podmiot przetwarzający,

b) kategorii przetwarzań dokonywanych w imieniu Administratora wynikających z celu świadczonych usług lub zawartej umowy powierzenia,

c) odnotowania faktu przekazania danych osobowych do państwa trzeciego,

d) ogólnego opisu technicznego i organizacyjnego środków bezpieczeństwa.

4.5. Rejestr czynności przetwarzania danych osobowych znajduje się w Załączniku nr 2 do niniejszej Polityki.

4.6. W przypadku istnienia więcej niż jednej bazy, dla której należy prowadzić rejestr kategorii czynności, dla każdej bazy prowadzony jest odpowiednio rejestr kategorii czynności przetwarzania, o którym mowa w rozdziale III pkt. 4.2.

4.7. Rejestr kategorii czynności przetwarzania danych Podmiotu przetwarzającego znajduje się w Załączniku nr 3 do niniejszej Polityki.

5. Inspektor ochrony danych osobowych

5.1. Funkcję Inspektora ochrony danych osobowych pełni osoba wskazana w rozdziale I pkt. 1 lit. i powyżej.

5.2. Inspektor ochrony danych osobowych i Administrator związani są umową o oświadczenie usług.

5.3. Inspektor ochrony danych realizuje zadania w zakresie ochrony danych osobowych, takie jak, w szczególności:

a) informowanie Administratora oraz jego pracowników i współpracowników o spoczywających na nim (nich) obowiązkach wynikających z RODO oraz innych przepisów UE lub przepisów krajowych,

b) bieżące doradztwo wobec Administratora oraz jego pracowników i współpracowników w zakresie stosowania przepisów dotyczących ochrony danych osobowych,

c) monitorowanie przestrzegania przepisów dotyczących ochrony danych osobowych oraz niniejszej Polityki, w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu Administratora uczestniczącego w operacjach przetwarzania oraz prowadzenie powiązanych z powyższym audytów bezpieczeństwa,

d) udzielanie na żądanie zaleceń co do oceny skutków przetwarzania danych osobowych dla ich ochrony oraz monitorowania jej wykonania,

e) współpraca z PUODO, w tym w razie potrzeby występowanie z uprzednimi konsultacjami w zakresie przetwarzania danych osobowych, oraz zgłaszanie naruszeń ochrony danych osobowych,

f) pełnienie funkcji punktu kontaktowego dla PUODO w kwestiach związanych z naruszeniem bezpieczeństwa przetwarzania danych osobowych,

g) pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą, w zakresie spełniania obowiązku informacyjnego oraz informowania o naruszeniach bezpieczeństwa przetwarzania danych osobowych.

5.4. Inspektor ochrony danych osobowych może pełnić swoje obowiązki z pomocą innych osób zatrudnionych lub niezatrudnionych przez Administratora.

5.5. W przypadku dłuższej nieobecności Inspektora ochrony danych osobowych jest on zobowiązany do wskazania osoby, która na czas jego nieobecności będzie zastępowała go w wykonywaniu jego obowiązków.

5.6. Inspektor ochrony danych osobowych realizuje zadania w zakresie ochrony danych osobowych, w szczególności poprzez następujące działania:

a) prowadzenie rejestru czynności przetwarzania danych osobowych i rejestru kategorii czynności przetwarzania danych osobowych Podmiotu przetwarzającego,

b) prowadzenie dokumentacji naruszeń ochrony danych osobowych,

c) nadzorowanie funkcjonowania mechanizmów uwierzytelniania użytkowników w systemie informatycznym służącym do przetwarzania danych osobowych oraz kontroli dostępu do danych osobowych,

d) nadzorowanie wykonywania kopii zapasowych (awaryjnych), ich przechowywanie oraz okresowe sprawdzanie pod kątem ich dalszej przydatności w zakresie odtwarzania danych osobowych w przypadku awarii systemu informatycznego,

e) nadzorowanie przestrzegania przez Administratora praw osób, których dane dotyczą,

f) podejmowanie stosownych działań zgodnie z niniejszą Polityką w sytuacji naruszenia ochrony danych osobowych, w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu informatycznego lub informacji o zmianach w sposobie działania systemu informatycznego, programów lub urządzeń wskazujących na naruszenie bezpieczeństwa danych osobowych,

g) przeglądanie niniejszej Polityki pod kątem jej aktualności i stosowania u Administratora, a w razie jej aktualizacji– kierowanie do Administratora stosownych zaleceń i wytycznych.

6. Pozostałe sposoby zabezpieczenia danych osobowych

6.1. Administrator zobowiązany jest do współpracy z PUODO.

6.2. Współpraca Administratora z PUODO może dotyczyć zgłaszania naruszeń, a także uprzednich konsultacji dotyczących właściwego przetwarzania danych osobowych.

6.3. W przypadku wystąpienia naruszenia bezpieczeństwa prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub winny sposób przetwarzanych Administrator danych osobowych zobowiązany jest do zawiadomienia PUODO w terminie 72 godzin po stwierdzeniu naruszenia.

6.4. Zgłoszenie naruszenia powinno zawierać/opisywać co najmniej:

a) charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,

b) imię i nazwisko oraz dane kontaktowe Inspektora ochrony danych osobowych lub oznaczenie punktu kontaktowego, od którego można uzyskać więcej informacji na temat naruszenia,

c) możliwe konsekwencje naruszenia ochrony danych osobowych,

d) środki zastosowane lub proponowane przez Administratora danych osobowych w celu zaradzenia na przyszłość naruszaniu ochrony danych osobowych, w tym– w stosownych przypadkach – planowane środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

6.5. Administrator danych osobowych zobowiązany jest zawiadomić bez zbędnej zwłoki osobę, której dane dotyczą, o każdym przypadku naruszenia ochrony danych jej dotyczących, szczególnie jeżeli incydent ten może powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

6.6. Zawiadomienie osoby, której dane dotyczą, musi zawierać/opisywać co najmniej:

a) imię i nazwisko oraz dane kontaktowe Inspektora ochrony danych osobowych lub oznaczenie punktu kontaktowego, który pozwoli uzyskać więcej informacji,

b) możliwe konsekwencje naruszenia ochrony danych osobowych,

c) środki zastosowane lub proponowane przez Administratora w celu zaradzenia naruszaniu ochrony danych osobowych, w tym– w stosownych przypadkach – środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

6.7. Zawiadomienie nie jest konieczne, jeżeli:

a) Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności chodzi o takie środki, jak pseudonimizacja (rozdział III pkt. 6.8.) oraz anonimizacja (rozdział III pkt. 6.9.) danych; stosowanie tych środków powoduje, że nawet naruszenie ochrony danych nie spowoduje powstania dodatkowego obowiązku informacyjnego (zawiadomienia),

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

c) wymagałoby ono niewspółmiernie dużego wysiłku; w takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

6.8. Administrator w celu zabezpieczenia stosuje technikę pseudonimizacji danych osobowych, polegającą na odwracalnym procesie, po którego przeprowadzeniu w przyszłości nie będzie możliwe zidentyfikowanie określonej osoby bez użycia dodatkowych informacji, pod warunkiem osobnego przechowywania tych dodatkowych informacji oraz zabezpieczenia ich odpowiednimi środkami technicznymi i organizacyjnymi uniemożliwiającymi przypisanie danych konkretnej osobie.

6.9. Administrator danych osobowych w miarę możliwości stosuje technikę anonimizacji danych osobowych, polegającą na nieodwracalnym procesie, po którego przeprowadzeniu w przyszłości nie będzie możliwe zidentyfikowanie określonej osoby na podstawie posiadanych przez Administratora informacji.

Rozdział IV
Transfer danych osobowych

1. Powierzenie do przetwarzania danych osobowych

1.1. Administrator danych osobowych dopuszcza możliwość przekazania danych osobowych do przetwarzania innym podmiotom przetwarzającym. W takim przypadku przetwarzanie danych osobowych odbywa się wyłącznie na podstawie umowy powierzenia przetwarzania danych osobowych zawartej pomiędzy Administratorem a Podmiotem przetwarzającym, zwanej dalej Umową- stanowiącą Załącznik 8 do niniejszej Polityki.

1.2. Umowa, o której mowa w punkcie poprzedzającym, musi być zawarta w formie pisemnej oraz zawierać ściśle określony zakres powierzonych do przetwarzania danych.

1.3. Przetwarzanie danych osobowych możliwe jest tylko w zakresie ustalonym przez Umowę.

1.4. Powierzone dane podlegają przetwarzaniu i ochronie na takich samych zasadach, jakie stosuje Administrator danych osobowych, chyba że Umowa określi inne zasady ochrony danych osobowych, pod warunkiem, że będą one zgodne z RODO.

1.5. Zmiana zasad związanych z ochroną danych osobowych oraz z ich przetwarzaniem przez Podmiot przetwarzający, któremu Administrator powierzył dane do przetwarzania, nie może:

a) naruszać praw osób, których dane są przetwarzane,

b) naruszać zasad związanych z ochroną danych osobowych przewidzianych w przepisach powszechnie obowiązujących,

c) zmieniać celu przetwarzania danych osobowych,

d) przetwarzać powierzonych danych osobowych w sposób inny niż taki, do którego upoważnił go Administrator danych osobowych,

e) udostępniać powierzonych danych osobowych osobom trzecim bez zgody Administratora.

1.6. Podmiot przetwarzający zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy w związku z przetwarzaniem powierzonych danych osobowych.

1.7. Podmiot przetwarzający:

a) zobowiązany jest zapewniać wszelkie środki wymagane do zapewnienia bezpieczeństwa przetwarzania danych osobowych,

b) w przypadku korzystania z podwykonawców przestrzega warunków korzystania z usług innego podmiotu przetwarzającego (w takim przypadku mamy do czynienia z tzw. podpowierzeniem przetwarzania danych osobowych),

c) pomaga Administratorowi danych osobowych za pomocą odpowiednich środków technicznych i organizacyjnych wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą,

d) po zakończeniu świadczenia usług związanych z przetwarzaniem – zależnie od decyzji Administratora – usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie,

e) udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków wynikających z powszechnie obowiązujących przepisów prawa, w tym w szczególności z RODO.

2. Udostępnianie danych osobowych

2.1. Administrator danych osobowych nie udostępnia przetwarzanych przez siebie danych osobowych innym administratorom, chyba że uzyska on zgodę osoby, której dane dotyczą, lub możliwość udostępnienia danych osobowych będzie wynikała z decyzji sądu, organu administracji publicznej lub nastąpi w oparciu o przepisy szczególne.

2.2. W przypadku udostępniania danych osobowych, poza odebraniem stosownych zgód od osób, których dane dotyczą, Administrator danych osobowych zobowiązany jest do zawarcia umowy dotyczącej udostępniania danych innym administratorom.

2.3. W przypadku udostępniania danych osobowych do państwa trzeciego Administrator danych osobowych zastosuje się do wymagań wynikających z przepisów powszechnie obowiązujących, a dotyczących udostępniania danych osobowych do państwa trzeciego.

2.4. W związku z udostępnianiem danych osobowych Administrator będzie zobowiązany do spełnienia obowiązku informacyjnego wobec osób, których dane będą udostępnione, polegającego na przekazaniu informacji dotyczącej:

a) tożsamości i danych kontaktowych Administratora danych osobowych oraz danych kontaktowych do IOD,

b) celów przetwarzania danych osobowych,

c) kategorii danych osobowych,

d) odbiorców danych osobowych,

e) ewentualnego przekazywania danych do państwa trzeciego,

f) okresu, przez który dane będą przetwarzane,

g) praw osoby, której dane dotyczą,

h) źródła danych osobowych,

i) profilowania (jeżeli ma to zastosowanie i zachodzi taka potrzeba).

Rozdział V
Opis zdarzeń naruszających ochronę danych osobowych

1. Możliwe zagrożenia dotyczące naruszenia ochrony danych osobowych

1.1. Podział zagrożeń:

a) **zagrożenia losowe zewnętrzne** – ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu informatycznego, a zatem ciągłość systemu informatycznego zostaje zakłócona, ale w przypadku takich zagrożeń nie dochodzi do naruszenia poufności danych, np. klęski żywiołowe, przerwy w zasilaniu itp.,

b) **zagrożenia losowe wewnętrzne** – ich występowanie może prowadzić do zniszczenia danych, zakłócenia ciągłości pracy systemu informatycznego oraz do naruszenia poufności danych, np. niezamierzone pomyłki operatorów, Administratora, Podmiotu przetwarzającego, awarie sprzętowe, błędy oprogramowania, pogorszenie jakości sprzętu i oprogramowania,

c) **zagrożenia zamierzone** – świadome i celowe działania powodujące naruszenie poufności danych, zazwyczaj nieskutkujące uszkodzeniem infrastruktury technicznej i zakłóceniem ciągłości pracy; zagrożenia te można podzielić na:

   – nieuprawniony dostęp do systemu informatycznego z zewnątrz (włamanie do wskazanych systemów),

   – nieuprawniony dostęp do systemu informatycznego z jego wnętrza,

   – nieuprawnione przekazanie danych,

   – bezpośrednie zagrożenie materialnych składników systemu informatycznego (np. kradzież sprzętu).

1.2. Naruszenie lub podejrzenie naruszenia systemu informatycznego, w którym przetwarzane są dane osobowe, następuje w sytuacji:

a) losowego lub nieprzewidzianego oddziaływania czynników zewnętrznych na zasoby systemu, jak np. wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne itp.,

b) niewłaściwych parametrów środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,

c) awarii sprzętu lub oprogramowania, które wyraźnie wskazuje na umyślne działanie w kierunku naruszenia ochrony danych,

d) pojawienia się odpowiedniego komunikatu alarmowego,

e) podejrzenia nieuprawnionej modyfikacji danych w systemie lub innego odstępstwa od stanu oczekiwanego,

f) naruszenia lub próby naruszenia integralności systemu lub bazy w tych systemach,

g) pracy w systemie wykazującej odstępstwa uzasadniające podejrzenie przełamania lub zaniechania ochrony danych osobowych, jak np. praca osoby, która nie jest formalnie dopuszczona do obsługi systemu,

h) ujawnienia nieautoryzowanych kont dostępu do systemu,

i) naruszenia dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (np. niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce itp.).

1.3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia fizycznego miejsc przechowywania i przetwarzania danych osobowych, jak np.:

a) niezabezpieczone pomieszczenia,

b) niezabezpieczone urządzenia archiwizujące,

c) pozostawianie danych w nieodpowiednich miejscach (m.in. w koszach na śmieci czy w miejscach publicznie dostępnych),

d) pozostawienie niezabezpieczonych dokumentów zawierających dane osobowe na stanowisku pracy w razie jego opuszczenia przez osobę przetwarzającą dane w imieniu Administratora.

Rozdział VI
System informatyczny i zabezpieczenie danych osobowych

1. Środki fizyczne

1.1. Administrator danych osobowych jest zobowiązany do zastosowania środków technicznych i organizacyjnych zapewniających optymalną ochronę przetwarzanych danych w systemie informatycznym, w tym w szczególności:

a) zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym,

b) zapobieganie przed pobraniem danych przez osobę nieuprawnioną,

c) zapobieganie zmianie, utracie, uszkodzeniu lub zniszczeniu danych,

d) zapewnianie przetwarzania danych zgodnie zobowiązującymi przepisami prawa.

1.2. Zadania określone w punkcie poprzedzającym wykonuje lub nadzoruje ich wykonanie w imieniu Administratora danych osobowych Inspektor ochrony danych osobowych i Administrator systemu.

1.3. Zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe:

a) dostęp do pomieszczeń, w których przetwarzane, a przede wszystkim przechowywane są dane osobowe, jest ograniczony wyłącznie do osób mających odpowiednie upoważnienie nadane przez Administratora danych osobowych,

b) pomieszczenia, w których przetwarza się, a przede wszystkim przechowuje się dane osobowe, zamykane są na klucz, na czas niekorzystania z ww. pomieszczeń,

c) w przypadku opuszczenia pomieszczenia przez ostatniego pracownika upoważnionego do przetwarzania danych osobowych – także w godzinach pracy – dane osobowe przechowywane w wersji tradycyjnej (papierowej) lub elektronicznej (na zewnętrznych nośnikach, np. pendrive, płyta CD/DVD) po zakończeniu pracy są przechowywane w miejscach zabezpieczonych przed dostępem nieupoważnionych osób trzecich; dodatkowo pracownik w razie opuszczania swojego stanowiska pracy zobowiązany jest do wylogowania się ze swojego komputera stacjonarnego/laptopa lub innego urządzenia mającego dostęp do systemu informatycznego,

d) nieaktualne lub błędne wydruki zawierające dane osobowe niszczone są w sposób uniemożliwiający odczyt danych, np. w niszczarkach,

e) budynek, w którym mieszczą się pomieszczenia służące do przetwarzania danych osobowych, posiada system alarmowy, system przeciwpożarowy, kontrolę wejścia/wyjścia (zeszyt wejść i wyjść), monitoring zewnętrzny i wewnętrzny, drzwi główne do budynku z kontrolą dostępu.

2. Środki techniczne

2.1. Nieautoryzowanemu dostępowi do bazy danych osobowych zapobiega stosowanie następujących zabezpieczeń:

a) podłączenie urządzenia końcowego (komputera, drukarki) do sieci telekomunikacyjnej dokonywane jest przez osobę upoważnioną przez Administratora danych osobowych,

b) udostępnianie każdemu Użytkownikowi zasobów sieci telekomunikacyjnej (programów i bazy danych osobowych) następuje na podstawie upoważnienia do przetwarzania danych osobowych,

c) identyfikacja każdego Użytkownika w systemie informatycznym następuje poprzez zastosowanie podwójnego uwierzytelnienia (tj. działania, którego celem jest weryfikacja deklarowanej tożsamości podmiotu korzystającego z systemu informatycznego),

d) każdemu Użytkownikowi przysługuje przydzielenie indywidualnego Identyfikatora do korzystania z systemu informatycznego,

e) klucze od pomieszczeń przetwarzania danych są udostępniane tylko upoważnionym pracownikom,

f) program antywirusowy z zaporą antywłamaniową jest używany na wszystkich urządzeniach, na których dochodzi do przetwarzania danych osobowych,

g) konta na urządzeniach wskazanych w literze poprzedzającej są zabezpieczone hasłami, a konta z ograniczonymi uprawnieniami używane są do ciągłej pracy,

h) monitory stanowisk przetwarzania danych osobowych są ustawione w sposób uniemożliwiający wgląd wdane osobom nieupoważnionym.

2.2. Przed nieautoryzowanym dostępem do bazy danych osobowych poprzez sieć telekomunikacyjną chronią następujące zabezpieczenia:

a) logiczne oddzielenie sieci lokalnej uniemożliwiające uzyskanie połączenia z bazą danych osobowych spoza systemu informatycznego, jak również uzyskanie dostępu z systemu informatycznego do sieci telekomunikacyjnej publicznej,

b) zastosowanie dwustopniowego zabezpieczenia sieci telekomunikacyjnej lokalnej:

   – lokalna brama sieciowa z zainstalowanym systemem typu firewall z funkcją analizy charakteru ruchu sieciowego, uniemożliwiającym nawiązanie połączenia do chronionych urządzeń i blokującym ruch o charakterystyce niepożądanej lub takiej, która może zostać uznana za szkodliwą.

2.3. Przed utratą danych osobowych w wyniku awarii chronią następujące zabezpieczenia:

a) ochrona sprzętu komputerowego przed zanikiem zasilania poprzez stosowanie listew przepięciowych,

b) ochrona przed utratą zgromadzonych danych poprzez cykliczne wykonywanie kopii zapasowych, z których w przypadku awarii odtwarzane są dane i system operacyjny (tzw. backupy),

c) zapewnienie właściwej temperatury i wilgotności powietrza dla pracy sprzętu komputerowego,

d) zwiększenie niezawodności serwerów i urządzeń sieciowych poprzez ich logiczne rozmieszczenie.

3. Procedury nadawania i zmiany uprawnień do przetwarzania danych

3.1. Każdy Użytkownik przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z niniejszą Polityką oraz zobowiązuje się ją bezwzględnie stosować.

3.2. Zapoznanie się z niniejszą Polityką Użytkownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi Załącznik nr 5 („Oświadczenie pracownika o zapoznaniu się z Polityką").

3.3. Zapoznanie powinno uwzględniać kilka zbiorów danych osobowych .

3.4. Administrator danych osobowych lub osoba przez niego upoważniona przyznaje uprawnienia w zakresie dostępu do przetwarzania danych, określając zakres uprawnień Użytkownika zgonie z Załącznikiem nr 4.

3.5. Ewidencja osób upoważnionych do przetwarzania danych osobowych, wskazująca konkretnych Użytkowników dopuszczonych do przetwarzania danych osobowych w określonych zbiorach, znajduje się w Załączniku nr 6 do niniejszej Polityki.

3.6. Ewidencja powinna uwzględniać upoważnienia do przetwarzania różnych zbiorów danych osobowych.

3.7. Administrator danych osobowych lub osoba przez niego upoważniona zakładają konto Użytkownika w systemie informatycznym o odpowiednim identyfikatorze i zabezpieczone hasłem.

3.8. Hasło uprawniające do korzystania z systemu informatycznego Użytkownik wpisuje osobiście.

3.9. Konto zostaje zablokowane lub usunięte przez Administratora danych osobowych lub osobę przez niego upoważnioną.

3.10. Hasła dostępu Użytkownika do systemu informatycznego stanowią tajemnicę służbową znaną wyłącznie temu Użytkownikowi.

3.11. Hasła, w stosunku do których zaistniało podejrzenie o ich ujawnieniu osobie nieuprawnionej, podlegają bezzwłocznej zmianie.

3.12. W celu zabezpieczenia awaryjnego dostępu do systemu informatycznego przetwarzającego dane osobowe aktualne hasło Administratora systemu posiada Administrator danych osobowych.

3.13. Pełne prawa Administratora systemu posiada tylko Administrator danych osobowych lub osoba przez niego upoważniona.

3.14. Podczas nieobecności osoby upoważnionej do wykonywania obowiązków Administratora systemu jego obowiązki wykonuje Administrator danych osobowych lub osoba przez niego upoważniona.

4. Rejestrowanie i usuwanie użytkowników z ewidencji osób dopuszczonych do przetwarzania danych osobowych

4.1. Osoba upoważniona przez Administratora danych osobowych do wykonywania obowiązków Administratora systemu prowadzi w imieniu Administratora ewidencję osób dopuszczonych do przetwarzania danych osobowych w oparciu o wnioski Administratora o przyznanie lub modyfikację uprawnień.

4.2. W przypadku otrzymania przez Inspektora ochrony danych osobowych, Administratora systemu lub inną osobę upoważnioną przez którykolwiek z tych podmiotów wniosku o zablokowanie lub usunięcie konta Użytkownika w systemie informatycznym jest on zobowiązany w trybie natychmiastowym odznaczyć ten fakt w „Ewidencji osób upoważnionych do przetwarzania danych osobowych", stanowiącej Załącznik nr 6 do niniejszej Polityki.

4.3. Konto Użytkownika usuwa Administrator systemu zgodnie ze szczegółowymi instrukcjami operacyjnymi specyficznymi dla danego systemu informatycznego.

4.4. Usunięcie konta z systemu informatycznego następuje na wniosek Administratora danych osobowych, Inspektora ochrony danych lub innej upoważnionej osoby.

5. Zasady posługiwania się hasłami

5.1. Bezpośredni dostęp do systemu informatycznego może mieć miejsce wyłącznie po podaniu identyfikatora Użytkownika i właściwego hasła.

5.2. Zmiana haseł Użytkowników w systemie informatycznym jest wymuszana przez wspomniany system w odpowiednich odstępach czasu, nie rzadziej niż co 90 dni.

5.3. Hasło Użytkownika powinno być zmieniane, szczególnie w sytuacjach, kiedy zaistnieje podejrzenie, że jest ono znane osobom nieupoważnionym.

5.4. Identyfikator Użytkownika nie może być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu Użytkownika z systemu informatycznego nie może on zostać przydzielony innej osobie.

5.5. Użytkownicy, w tym w szczególności pracownicy, są odpowiedzialni za zachowanie poufności swoich identyfikatorów i haseł.

5.6. Hasła Użytkowników utrzymuje się w tajemnicy również po upływie ich ważności.

5.7. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie. W sytuacji, kiedy zachodzi podejrzenie, że osoba nieupoważniona poznała hasło w sposób nieuprawniony, Użytkownik zobowiązany jest do natychmiastowej zmiany hasła i poinformowania o zaistniałym fakcie Administratora systemu i Inspektora ochrony danych osobowych.

5.8. Przy wyborze hasła obowiązują następujące zasady:

a) minimalna długość hasła to6 znaków;

b) zakazuje się stosowania:
   - haseł, które Użytkownik stosował uprzednio,
   - swojego Identyfikatora w jakiejkolwiek formie,
   - swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiejkolwiek formie, imion (w szczególności imion osób z najbliższej rodziny),
   - ogólnie dostępnych informacji o Użytkowniku (numer telefonu, numer rejestracyjny samochodu, numer PESEL itp.),

c) należy stosować:
   - hasła zawierające kombinacje liter (małych i dużych) i cyfr arabskich,
   - hasła zawierające znaki specjalne: (.,();'@, #, & itp.), o ile system informatyczny i oprogramowanie na to pozwalają;

d) zmiany hasła nie wolno zlecać innym osobom.

6. Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym

6.1. Rozpoczęcie pracy w systemie informatycznym na komputerach wymaga zalogowania przy użyciu indywidualnego identyfikatora oraz hasła.

6.2. Przed opuszczeniem stanowiska pracy należy zablokować stację roboczą lub wylogować się z oprogramowania i systemu informatycznego.

6.3. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów, wylogować się z systemu informatycznego.

6.4. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania.

7. Procedury tworzenia kopii zapasowych

7.1. Za systematyczne przygotowanie kopii bezpieczeństwa odpowiada Administrator systemu pod nadzorem Administratora danych osobowych.

7.2. Kopie bezpieczeństwa są wykonywane codziennie przez administrację serwera, na którym gromadzone są dane, jeżeli do gromadzenia danych dochodzi na tym serwerze.

7.3. W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom nieuprawnionym. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, ulegają zniszczeniu w stopniu uniemożliwiającym ich odczytanie, przede wszystkim za pomocą niszczarek.

8. Sposób zabezpieczenia systemu informatycznego przed wirusami i szkodliwym oprogramowaniem

8.1. Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe z włączoną ochroną antywirusową i antyspyware.

8.2. Każdy e-mail wpływający na konta pocztowe musi być sprawdzony pod kątem występowania wirusów przez oprogramowanie antywirusowe.

8.3. Definicje wzorców wirusów aktualizowane są nie rzadziej niż raz w tygodniu.

8.4. Bezwzględnie zabrania się używania nośników niewiadomego pochodzenia.

8.5. Bezwzględnie zabrania się pobierania z sieci telekomunikacyjnej plików niewiadomego pochodzenia.

8.6. Administrator systemu przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach, na których przetwarzane są dane osobowe, w tym co najmniej raz na jeden miesiąc.

8.7. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe, na którym wykryto wirusa, oraz wszystkie posiadane przez Użytkownika nośniki.

9. Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych

9.1. Dane osobowe przetwarzane z użyciem systemów informatycznych mogą być udostępniane wyłącznie osobom uprawnionym wpisanym do ewidencji osób dopuszczonych do przetwarzania danych osobowych w systemie informatycznym.

9.2. Udostępnianie danych osobowych nie może być realizowane drogą telefoniczną.

9.3. System informatyczny oraz aplikacje wykorzystywane do obsługi bazy danych osobowych zapewniają odnotowanie informacji i ich przekazanie odbiorcom danych. Zakres informacji powinien obejmować co najmniej dane odbiorcy, datę przekazania oraz zakres udostępnionych danych.

10. Procedury wykonywania przeglądów i konserwacji systemu informatycznego

10.1. Przeglądy i konserwacja urządzeń:

a) przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonych przez producenta sprzętu,

b) nieprawidłowości ujawnione w trakcie tych działań powinny być niezwłocznie usunięte, ich przyczyny przeanalizowane, a o fakcie ujawnienia nieprawidłowości Administrator systemu jest obowiązany zawiadomić Administratora danych osobowych oraz Inspektora ochrony danych osobowych.

10.2. Przegląd programów i narzędzi programowych składających się na system informatyczny, w tym m.in. konserwacja bazy danych osobowych, jest przeprowadzany zgodnie z zaleceniami twórców poszczególnych programów.

10.3. W przypadku przekazania do naprawy nośników informatycznych zawierających dane osobowe lub sprzętu komputerowego, którego nośniki mogą zawierać dane osobowe, należy wcześniej wskazać sposób usuwania (tj. zniszczenia, usunięcia danych osobowych lub taką ich modyfikację, w tym pseudonimizację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą) danych osobowych z tych nośników.

11. Połączenie do sieci telekomunikacyjnej

11.1. Połączenie do sieci telekomunikacyjnej jest realizowane przez sieć przewodową lub bezprzewodową z zastosowaniem następujących zasad ochrony:

a) dostęp do sieci telekomunikacyjnej wymaga podania klucza składającego się z liter i cyfr oraz zezwolenia na zalogowanie się do sieci przez Administratora systemu,

b) każdy komputer posiadający dostęp do sieci telekomunikacyjnej posiada oprogramowanie antywirusowe chroniące przed złośliwym oprogramowaniem (antyspyware) oraz zaporę sieciową (firewall),

c) osobie korzystającej z sieci telekomunikacyjnej zabrania się wchodzenia na strony niezgodne z prawem lub rozsiewające wirusy oraz programy szpiegujące (trojan, spyware).

11.2. Połączenie z siecią telekomunikacyjną publiczną zabezpieczone jest przez moduł firewall działający na routerze sieciowym.

11.3. Na każdym komputerze w systemie informatycznym działa osobny firewall.

11.4. Zabronione jest połączenie z siecią telekomunikacyjną z niedziałającym programem antywirusowym i firewallem lub w przypadku ich braku.

12. Korzystanie z komputerów i urządzeń przenośnych

12.1. Administrator danych osobowych oraz Inspektor ochrony danych osobowych dopuszcza korzystanie z komputerów i urządzeń przenośnych, w tym tabletów oraz smartfonów.

12.2. Komputery przenośne (laptopy), używane do przetwarzania danych osobowych, zabezpieczone są podczas transportu oraz przechowywania przed dostępem do tych danych osób nieuprawnionych, w szczególności:

a) dostęp do komputerów przenośnych zabezpieczony jest przez identyfikator i hasło,

b) nie zezwala się na używanie komputera przenośnego osobom nieupoważnionym do dostępu do danych osobowych,

c) pliki zdanymi osobowymi dostępne na komputerze przenośnym są zaszyfrowane bądź chronione hasłem.

12.3. Postanowienia punktu poprzedzającego stosuje się odpowiednio do urządzeń przenośnych, w tym tabletów i smartfonów, o których mowa w rozdziale VI pkt. 12.1.,

przy czym zasady, o których mowa w rozdziale VI pkt. 5.8., mają zastosowanie w zakresie możliwości technicznych urządzenia przenośnego.

Rozdział VII
Kontrola przestrzegania zasad zabezpieczenia danych osobowych

1. Inspektor ochrony danych osobowych sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikający z przepisów powszechnie obowiązujących, w tym w szczególności z RODO, oraz zasad ustanowionych w niniejszej Polityce.

2. Inspektor ochrony danych osobowych przeprowadza kontrole monitorujące przestrzeganie ochrony danych osobowych w terminach uzgodnionych z Administratorem. Monitorowanie podlega udokumentowaniu.

Rozdział VIII
Postępowanie w przypadku naruszenia ochrony danych osobowych

1. W przypadku stwierdzenia naruszenia:

a) zabezpieczenia systemu informatycznego,

b) technicznego stanu urządzeń,

c) zawartości zbiorów danych osobowych,

d) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,

e) innych zdarzeń mogących mieć wpływ na naruszenie ochrony danych osobowych (np. zalanie, pożar, kradzież itp.)

każda osoba zatrudniona lub współpracująca z Administratorem danych osobowych zobowiązana jest do niezwłocznego powiadomienia o tym fakcie Administratora danych osobowych, Inspektora ochrona danych osobowych i swojego bezpośredniego przełożonego.

2. Po wykryciu zdarzeń określonych w punkcie poprzedzającym należy:

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

b) rozważyć wstrzymanie bieżącej pracy na komputerze w celu zabezpieczenia miejsca zdarzenia,

c) zaniechać – o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę zdarzenia,

d) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu informatycznego, aplikacji użytkowej lub winnym właściwym dokumencie,

e) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,

f) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora danych osobowych, jego przedstawiciela lub innej osoby upoważnionej, a w miarę możliwości również Inspektora ochrony danych osobowych.

3. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych Administrator danych osobowych, jego przedstawiciel lub osoba przez niego upoważniona:

a) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania, mając na uwadze ewentualne zagrożenia dla prawidłowości pracy,

b) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,

c) w razie potrzeby powiadamia o zaistniałym naruszeniu Inspektora ochrony danych osobowych, jeżeli nie był obecny na miejscu zdarzenia,

d) jeżeli zachodzi taka potrzeba, zleca usunięcie występujących naruszeń,

e) jeżeli zachodzi taka potrzeba, w terminie 72 godzin powiadamia PUODO o zaistniałym naruszeniu,

f) jeżeli zachodzi taka potrzeba i nie występują przesłanki, które wykluczają konieczność powiadomienia, bez zbędnej zwłoki powiadamia osoby, których dane dotyczą, o wystąpieniu naruszenia.

4. Administrator danych osobowych, Inspektor ochrony danych osobowych lub osoba upoważniona przez którykolwiek z tych podmiotów dokumentuje zaistniały przypadek naruszenia, sporządzając stosowną notatkę w oparciu o przeprowadzone bezpośrednio czynności lub w oparciu o uzyskane informacje.

5. Zaistniałe naruszenie może stać się przedmiotem szczegółowej analizy prowadzonej przez Administratora danych osobowych i Inspektora ochrony danych osobowych.

6. Analiza, o której mowa w rozdziale VIII pkt. 4, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie osób odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

7. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszej Polityce, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, wszczyna się postępowanie dyscyplinarne.

8. Administrator danych osobowych prowadzi dokumentację naruszeń ochrony danych osobowych, zgodnie z Załącznikiem nr 7 do niniejszej Polityki ochrony danych osobowych.

Rozdział IX
Postanowienia końcowe

Niniejsza Polityka ochrony danych osobowych obowiązuje od dnia 3 września 2018r. Wszelkie zmiany procedur wynikających z niniejszej Polityki wymagają zatwierdzenia przez Administratora danych osobowych oraz Inspektora ochrony danych osobowych.

Administrator danych osobowych

Spis załączników „Polityki bezpieczeństwa i ochrony danych osobowych”:

Załącznik nr 1. Obszary przetwarzania i wykaz środków technicznych

Załącznik nr 2. Rejestr czynności przetwarzania danych osobowych.

Załącznik nr 3. Rejestr kategorii czynności przetwarzania danych Podmiotu przetwarzającego

Załącznik nr 4. Upoważnienie do przetwarzania danych

Załącznik nr 5. Oświadczenie pracownika o zapoznaniu się z Polityką

Załącznik nr 6. Ewidencja osób upoważnionych do przetwarzania danych osobowych

Załącznik nr 7. Dokumentacja naruszenia ochrony danych osobowych

Załącznik nr 8. Umowa powierzenia danych osobowych