

Zarządzenie nr 19/2026
Dyrektora Miejskiego Centrum Kultury Sportu i Rekreacji
im. Ryszarda Kaczorowskiego w Raciążu
z 15.10.2026 roku
w sprawie przyjęcia polityki ochrony danych osobowych

Dyrektor Miejskiego Centrum Kultury Sportu i Rekreacji im. Ryszarda Kaczorowskiego w Raciążu w związku z art. 24 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 2016, Nr 119, s. 1) zarządza się, co następuje:

§1

Przyjmuje się politykę ochrony danych osobowych, która stanowi załącznik do niniejszego zarządzenia.

§2

Przyjmuje się wyliczone ryzyko znajdujące się w rejestrze czynności przetwarzania. Ryzyko zostało wyliczone na podstawie dokumentu „Analiza zagrożeń i ryzyka”.

§3

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
Miejskiego Centrum Kultury, Sportu i Rekreacji
im. Ryszarda Kaczorowskiego w Raciążu

Robert Szymborski

Załącznik
do zarządzenia nr 19/2026
Dyrektora Miejskiego Centrum Kultury Sportu i Rekreacji
im. Ryszarda Kaczorowskiego w Raciążu
z 15.10.2026 r.
w sprawie przyjęcia polityki ochrony danych osobowych

**POLITYKA
OCHRONY DANYCH OSOBOWYCH**
*Miejskiego Centrum Kultury Sportu i Rekreacji
im. Ryszarda Kaczorowskiego w Raciążu*



Spis treści

<i>Spis treści</i>	2
A. ZASADY OGÓLNE	4
I. PODSTAWY PRAWNE	4
II. PODSTAWOWE POJĘCIA	4
III. CELE I ZASADY FUNKCJONOWANIA POLITYKI OCHRONY DANYCH OSOBOWYCH	4
IV. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH	5
V. OBOWIĄZEK ZACHOWANIA POUFNOŚCI I OCHRONY DANYCH OSOBOWYCH	7
VI. DOPUSZCZENIE UŻYTKOWNIKA DO PRZETWARZANIA DANYCH OSOBOWYCH	7
VII. POSTĘPOWANIE DYSCIPLINARNE	8
VIII. OBOWIĄZEK INFORMACYJNY I WYRAŻENIE ZGODY	8
IX. PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ	8
X. PROCEDURA REALIZACJI PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ	9
B. ZASADY DLA UŻYTKOWNIKÓW – ZABEZPIECZENIA FIZYCZNE	11
XI. ZABEZPIECZENIE DOKUMENTACJI PAPIEROWEJ Z DANymi OSOBOWymi	11
XII. POLITYKA KLUCZY	11
C. ZASADY DLA UŻYTKOWNIKÓW - IT	12
XIII. BEZPIECZNE UŻYTKOWANIE SPRZĘTU IT, DYskÓW, PROGRAMÓW	12
XIV. KORZYSTANIE Z USŁUG OPARTYCH NA SZTUCZNEJ INTELIGENCJI	13
XV. WYKORZYSTANIE BIOMETRII DO ZABEZPIECZENIA SPRZĘTU SŁUŻBOWEGO	14
XVI. BEZPIECZEŃSTWO WYMIENNYCH NOŚNIKÓW INFORMACJI	14
XVII. ZARZĄDZANIE UPRAWNIENIAMI	15
XVIII. POLITYKA HASEŁ	15
XIX. KORZYSTANIE Z INTERNETU	16
XX. KORZYSTANIE Z POCZTY ELEKTRONICZNEJ	16
XXI. OCHRONA ANTYWIRUSOWA	17
D. ZASADY DLA ADMINISTRATORA – IT	17
XXII. WYKONYWANIE PRZEGLĄDÓW, KONSERWACJI, NAPRAW SPRZĘTU IT, SYSTEMÓW SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH	17
XXIII. TWORZENIE KOPII ZAPASOWYCH	18
XXIV. ZARZĄDZANIE ZMIANĄ W SYSTEMIE, KTÓRY JEST WŁASNOŚCIĄ ADMINISTRATORA (USŁUGA WŁASNA)	18
XXV. ZARZĄDZANIE ZMIANĄ W SYSTEMIE, KTÓRY JEST WŁASNOŚCIĄ ADMINISTRATORA (ADMINISTRATOR KORZYSTA ZE WSPARCIA PODMIOTU ZEWNĘTRZNEGO – WDRAŻANIE I KOORDYNACJA SYSTEMU – PODMIOT PRZETWARZAJĄCY)	19
XXVI. ZARZĄDZANIE ZMIANĄ W SYSTEMIE, KTÓRY NIE JEST WŁASNOŚCIĄ ADMINISTRATORA (ADMINISTRATOR KORZYSTA ZE WSPARCIA PODMIOTU – PODMIOT PRZETWARZAJĄCY)	20
XXVII. MONITORING WIZYJNY	20
E. ZASADY DLA ADMINISTRATORA – OGÓLNE	21
XXVIII. PROJEKTOWANIE PRYWATNOŚCI	21
XXIX. IDENTYFIKACJA OBSZARÓW WYMAGAJĄCYCH SZCZEGÓLNYCH ZABEZPIECZEŃ	21
XXX. ANALIZA ZAGROZEŃ I RYZYKA	21
XXXI. OCENA SKUTKÓW DLA OCHRONY DANYCH (DPiA)	22
XXXII. TESTOWANIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH	22
F. NARUSZENIA OCHRONY DANYCH OSOBOWYCH	22
XXXIII. POSTĘPOWANIE NA WYPADEK WYSTĄPIENIA NARUSZENIA OCHRONY DANYCH	22
XXXIV. ANALIZA WYSTĄPIENIA RYZYKA NARUSZENIA PRAW I WOLNOŚCI OSÓB FIZYCZNYCH	23
G. PRZEKAZYWANIE DANYCH OSOBOWYCH	24
XXXV. UDOSTĘPNIANIE I POWIERZANIE DANYCH OSOBOWYCH	25
XXXVI. WSPÓŁADMINISTROWANIE DANymi OSOBOWymi	25

XXXVII.	POSTĘPOWANIE, GDY ADMINISTRATOR WYSTĘPUJE JAKO PODMIOT PRZETWARZAJĄCY	25
XXXVIII.	TRANSFER DANYCH POZA EUROPEJSKI OBSZAR GOSPODARCZY	26
H.	ZAŁĄCZNIKI	27



A. ZASADY OGÓLNE

I. Podstawy prawne

- 1st 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).
- 2nd Ustawa z 10 maja 2018 r. o ochronie danych osobowych.

II. Podstawowe pojęcia

- 1st Administrator (ADO) – w tym dokumencie jest rozumiany jako Miejskie Centrum Kultury Sportu i Rekreacji im. Ryszarda Kaczorowskiego w Raciążu.
- 2nd RODO/Rozporządzenie – w tym dokumencie rozumiane jako 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).
- 3rd Polityka – w tym dokumencie jest rozumiana jako „Polityka Ochrony Danych Osobowych” obowiązująca u Administratora.
- 4th Inspektor Ochrony Danych (IOD) – osoba wyznaczona przez Administratora do nadzorowania przestrzegania zasad ochrony danych osobowych oraz przygotowania dokumentów wymaganych przez RODO. IOD powołany jest zarządzeniem Dyrektora Administratora.
- 5th Dane osobowe – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
- 6th Użytkownik – w tym dokumencie osoba upoważniona do przetwarzania danych osobowych. Użytkownikiem może być m.in. osoba zatrudniona, wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, porozumienia wolontarystycznego, odbywająca staż, praktyki.
- 7th AI – rozumie się przez to sztuczną inteligencję.
- 8th Transfer danych – przekazanie lub umożliwienie dostępu do danych osobowych odbiorcy w Państwie Trzecim.

III. Cele i zasady funkcjonowania Polityki ochrony danych osobowych

- 1st Niniejsza Polityka obowiązuje wszystkich użytkowników w trakcie wykonywania obowiązków służbowych zarówno w pomieszczeniach służbowych jak i w innych miejscach np. w trakcie pracy zdalnej, odbywania podróży służbowych itp.
- 2nd Jeśli Administrator wyraża zgodę na używanie sprzętu prywatnego do celów służbowych użytkownik zobowiązany jest do zabezpieczenia sprzętu prywatnego zgodnie z obowiązującą Polityką u Administratora.
- 3rd Realizując Politykę ochrony danych osobowych zapewnia się ich:
- 1) poufność – informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, podmiotom i procesom;
 - 2) integralność – dane nie zostają zmienione lub zniszczone w sposób nieautoryzowany;
 - 3) dostępność – istnieje możliwość wykorzystania ich na żądanie, w założonym czasie, przez autoryzowany podmiot;
 - 4) rozliczalność – możliwość jednoznacznego przypisania działań poszczególnym osobom;
 - 5) autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana;
 - 6) niezaprzeczalność – uczestnictwo w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne;
 - 7) niezawodność – zamierzone zachowania i skutki są spójne;
 - 8) minimalizację – zbieranie jak najmniej danych osobowych i tylko takich jakie są wymagane do realizacji zadań Administratora.
- 4th Polityka ma na celu zredukowanie możliwości wystąpienia negatywnych konsekwencji naruszeń w tym

zakresie, to jest:

- 1) naruszeń danych osobowych rozumianych jako prywatne dobro powierzone;
- 2) naruszeń przepisów prawa oraz innych regulacji;
- 3) utraty lub obniżenia reputacji;
- 4) strat finansowych ponoszonych w wyniku nałożonych kar.

5th Realizując politykę w zakresie ochrony danych osobowych Administrator dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:

- 1) przetwarzane zgodnie z prawem;
- 2) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami;
- 3) merytorycznie poprawne i adekwatne w stosunku do celu, w jakim są przetwarzane;
- 4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

IV. Zasady przetwarzania danych osobowych

1. Administrator przestrzega następujących zasad przetwarzania danych osobowych:

1) Zasada zgodności z prawem, rzetelności i przejrzystości:

Komunikaty związane z przetwarzaniem danych osobowych są łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem. Informacje te są przekazywane pośrednio w formie elektronicznej za pomocą stron internetowych. Ponadto Administrator w sposób bezpośredni powiadamia osoby, których dane dotyczą, wysyłając do nich bezpośrednio w formie tradycyjnej papierowej lub w formie elektronicznej klauzule informacyjne, w których podaje informacje przewidziane w Rozporządzeniu. Administrator podaje te informacje zarówno w przypadku zbierania danych od osoby, której dane dotyczą, jak i w przypadku zbierania danych w sposób inny niż od osoby, której dane dotyczą. Administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania każdego odbiorcę, któremu ujawnił dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

2) Zasada ograniczenia celu przetwarzania danych:

Dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach, wynikających z działań statutowych Administratora i nieprzetwarzane dalej niezgodnie z tymi celami. Osoby, których dane dotyczą, są informowane o celach przetwarzania, zgodnie z zasadami i w sposób określony w pkt. 1. powyżej. Administrator, w sytuacji, gdy planuje przetwarzać dane w innym celu niż zostały zebrane, wysyła przed dalszym przetwarzaniem stosowną informację do osoby, której dane dotyczą i dostarcza jej wszystkich niezbędnych informacji w tym zakresie. Administrator może podjąć decyzję, że dane osobowe będą przetwarzane do celów archiwalnych i statystycznych.

3) Zasada minimalizacji danych:

Dane osobowe przetwarzane są w sposób i w czasie niezbędnym do celów, w których są przetwarzane. Celami Administratora są jego prawnie uzasadnione cele wyrażające się w jego działalności statutowej. Administrator dokonuje okresowo selekcji danych i wybiera tylko taką ilość danych, jaka jest dla niego niezbędna do realizacji celów statutowych.

4) Zasada prawidłowości danych:

Administrator zapewnia prawidłowość i aktualność danych. Każda osoba, której dane dotyczą, może zgłosić Administratorowi prośbę o poprawienie, uaktualnienie, sprostowanie danych, a także usunięcie danych, które są nieprawidłowe. Po zgłoszeniu użytkownicy Administratora do tego upoważnieni dokonują poprawienia, aktualizacji, sprostowania lub usunięcia nieprawidłowych danych w zbiorze danych.

5) Zasada ograniczenia przechowania danych:

Dane osobowe są adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane. Celem Administratora jest realizacja prawnie uzasadnionego celu, tj. jego celów statutowych. Działalność Administratora jest nieograniczona w czasie. Dlatego też Administrator nie określa czasu przechowania danych. Wdraża natomiast procedurę okresowego przeglądu danych i wybiera tylko taką ilość danych, jaka jest dla niego niezbędna do realizacji celów statutowych.

6) Zasada integralności i poufności danych:



Dane osobowe są przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu. Służą temu rozwiązania organizacyjne i techniczne stosowane przez Administratora a opisane w niniejszej Polityce.

7) Zasada rozliczalności:

Administrator wykazuje przestrzeganie zasad przetwarzania danych osobowych poprzez:

- a) informacje dla osób, których dane są przetwarzane na stronach internetowych;
- b) informacje dla osób, których dane są przetwarzane przekazywane w sposób bezpośredni w formie elektronicznej lub papierowej w formie klauzul informacyjnych;
- c) możliwość uzyskania przez każdą osobę w powszechnie używanym formacie jej danych osobowych;
- d) możliwość uzyskania informacji dotyczących danych osobowych na specjalnie przeznaczonych do tego skrzynkach pocztowych;
- e) dokumentowanie obsługi obowiązków informacyjnych, zawiadomień i żądań osób, których dane dotyczą;
- f) rejestr czynności przetwarzania danych dokumentujący podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania;
- g) rejestr kategorii czynności przetwarzania danych osobowych;
- h) upoważnienia do przetwarzania danych osobowych; wzór upoważnienia stanowi załącznik nr 1 do niniejszej Polityki;
- i) ewidencję osób upoważnionych do przetwarzania danych osobowych; wzór ewidencji stanowi załącznik nr 2 do niniejszej Polityki;
- j) oświadczenia o zachowaniu poufności; wzór oświadczenia stanowi załącznik nr 3 do niniejszej Polityki;
- k) umowy z podmiotami, którym powierzono przetwarzanie danych, w tym rejestr zawartych umów; wzór rejestru stanowi załącznik nr 6 do niniejszej Polityki. Administrator aktualizuje rejestr dwa razy w roku;
- l) inne rozwiązania organizacyjne i techniczne, określone w załącznikach do niniejszej Polityki oraz innych wewnętrznych regulacji.

8) Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach:

- a) Administrator nie podejmuje decyzji w indywidualnych przypadkach, które opierają się wyłącznie na zautomatyzowanym przetwarzaniu;
 - b) Administrator stosuje i wdraża zasady Privacy by Design (zasady prywatności w fazie projektowania) i Privacy by Default (zasady domyślnej ochrony danych osobowych) na każdym etapie przetwarzania danych. Oznacza to, że:
 - ochrona prywatności jest uwzględniana już na etapie projektowania systemów, procesów i usług związanych z przetwarzaniem danych osobowych;
 - domyślne ustawienia systemów i aplikacji zapewniają najwyższy poziom ochrony danych osobowych, minimalizując ich zakres przetwarzania i dostępność tylko dla osób upoważnionych;
 - wdrożone środki organizacyjne i techniczne zapewniają bezpieczeństwo oraz zgodność z przepisami o ochronie danych osobowych, w tym z RODO;
 - regularnie przeprowadzane są analizy ryzyka i oceny skutków dla ochrony danych, aby dostosować środki bezpieczeństwa do zmieniających się zagrożeń;
 - wszystkie osoby uczestniczące w procesie przetwarzania danych osobowych są szkolone w zakresie zasad ochrony prywatności i stosowania najlepszych praktyk.
2. Administrator stosuje w obszarach, w których jest to niezbędne, proces pseudonimizacji, polegający na przekształceniu danych w sposób, który uniemożliwia ich bezpośrednie powiązanie z konkretną osobą bez użycia dodatkowych informacji. Dodatkowe informacje niezbędne do identyfikacji osoby są przechowywane oddzielnie i podlegają ścisłym mechanizmom bezpieczeństwa, zapobiegającym ich nieautoryzowanemu wykorzystaniu. Proces pseudonimizacji stosowany jest zgodnie z obowiązującymi przepisami o ochronie danych osobowych oraz dobrą praktyką w zakresie bezpieczeństwa informacji.

V. Obowiązek zachowania poufności i ochrony danych osobowych

- 1st Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego.
- 2nd Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.
- 3rd Na podstawie art. 30 ust. 4 RODO w związku z art. 4 pkt 21 RODO zabrania się udostępniania rejestru czynności przetwarzania danych osobowych innym podmiotom niż organowi nadzorcemu, którym jest Prezes Urzędu Ochrony Danych Osobowych.
- 4th W przypadku gdy podmiot jest podmiotem przetwarzającym (np. w ramach projektu realizowanego ze środków europejskich) dozwolone jest częściowe udostępnienie rejestru kategorii czynności przetwarzania danych osobowych, ale wyłącznie w zakresie fragmentu dotyczącego kontrolowanej czynności.
- 5th Korespondencja zawierająca dane osobowe dłużnika nie może być dostarczana do skrzynki pocztowej, gdyż istnieje ryzyko, że dostęp do danych w niej zawartych może uzyskać osoba, do której korespondencja nie była skierowana. Taką korespondencję należy dostarczać dłużnikowi do rąk własnych.
- 6th W przypadku znalezienia danych osobowych (w postaci elektronicznej lub papierowej), powinny być one przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność. Dodatkowo przetwarzanie tych danych powinno odbywać się w sposób gwarantujący ochronę przed nieuprawnionym dostępem.
- 7th Anonimizacji dokumentów w formie papierowej i elektronicznej należy dokonywać zgodnie z procedurą opisaną w załączniku nr 13.

VI. Dopuszczenie użytkownika do przetwarzania danych osobowych

- 1st Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
 - 1) przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora zadaniach;
 - 2) zachowania w tajemnicy danych osobowych, do których ma lub będzie mieć dostęp w związku z wykonywaniem zadań powierzonych przez Administratora;
 - 3) niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Administratora;
 - 4) zachowania w tajemnicy sposobów zabezpieczenia danych osobowych;
 - 5) ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.
- 2nd Do przetwarzania danych osobowych mogą mieć dostęp jedynie osoby posiadające pisemne upoważnienie do przetwarzania danych osobowych nadane przez Administratora.
- 3rd Dyrektor przygotowuje upoważnienie do przetwarzania danych osobowych wg wzoru stanowiącego załącznik nr 1 do niniejszej Polityki.
- 4th Upoważnienie przygotowuje się w 2 egzemplarzach. Jeden egzemplarz włącza się do akt osobowych, drugi egzemplarz przekazuje się pracownikowi.
- 5th W przypadku zmiany stanowiska lub zakresu obowiązków osoby upoważnionej albo w przypadku wystąpienia innych okoliczności, które wpływają bezpośrednio na rodzaj i zakres przetwarzanych danych osobowych, Dyrektor przygotowuje nowe upoważnienie do przetwarzania danych osobowych.
- 6th Dyrektor prowadzi ewidencję wydanych upoważnień wg wzoru stanowiącego załącznik nr 2 do niniejszej Polityki.
- 7th W przypadku ustania zatrudnienia lub zaistnienia innej przyczyny skutkującej odwołaniem upoważnienia Dyrektor odnotowuje zmiany w ewidencji osób upoważnionych do przetwarzania danych osobowych.
- 8th Osoba dopuszczona do przetwarzania danych osobowych musi zostać przeszkolona z zasad ochrony danych osobowych, przed wydaniem upoważnienia do przetwarzania danych osobowych. W szkoleniu przypominającym należy wziąć udział minimum raz w roku.
- 9th Osoby zapoznane z treścią niniejszej Polityki oraz przeszkolone zobowiązane są podpisać oświadczenie o poufności, które stanowi załącznik nr 3.

VII. Postępowanie dyscyplinarne

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez Administratora za naruszenie przepisów zawartych w RODO.

VIII. Obowiązek informacyjny i wyrażenie zgody

- 1st Każdy użytkownik, który zbiera dane osobowe w imieniu Administratora, jest zobowiązany do przekazania zainteresowanemu obowiązkowi informacyjnego.
- 2nd Dedykowany obowiązek informacyjny powinien być zamieszczony w każdym miejscu, gdzie są zbierane dane osobowe (np. na stronie internetowej, w postępowaniu przetargowym, w formularzach zgłoszeniowych).
- 3rd Zaleca się, by obowiązek informacyjny oraz zgoda na przetwarzanie danych osobowych była, o ile to możliwe, zawsze podpisana przez osobę, której dane dotyczą lub potwierdzona elektronicznie.
- 4th Jeżeli dane osobowe zostały pozyskane w inny sposób niż od osoby, której dane dotyczą, obowiązek informacyjny należy przedstawić tej osobie:
 - 1) w rozsądnym terminie po uzyskaniu danych osobowych – najpóźniej w ciągu miesiąca;
 - 2) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji, z tą osobą, nie później niż w ciągu miesiąca;
 - 3) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu, nie później niż w ciągu miesiąca.
- 5th Użyte w art. 81 ust. 2 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych „zgromadzenie” jest pojęciem ocennym, które należy interpretować w oparciu o dany stan faktyczny. Rozpowszechnianie wizerunku danej osoby nie wymaga wyrażenia przez nią zgody, jeśli stanowi on jedynie element akcydentalny lub akcesoryjny przedstawionej całości, tzn. w razie usunięcia wizerunku nie zmieniłyby się przedmiot i charakter przedstawienia.

IX. Prawa osób, których dane dotyczą

- 1st Osoba, której dane dotyczą przetwarzane przez Administratora dane osobowe, ma prawa wynikające z Rozporządzenia.
- 2nd Prawo dostępu do danych – uprawnienie do uzyskania od Administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeśli to ma miejsce, osoba jest uprawniona do uzyskania dostępu do nich.
- 3rd Prawo do sprostowania danych – uprawnienie do niezwłocznego sprostowania przez Administratora danych osobowych osoby, które nie są prawidłowe lub uzupełnienia niekompletnych danych osobowych.
- 4th Prawo do usunięcia danych ("prawo do bycia zapomnianym") – uprawnienie do wniesienia żądania niezwłocznego usunięcia danych osobowych, jeśli zachodzi jedna z przesłanek:
 - 1) dane osobowe nie są już niezbędne do celów, w których zostały zebrane;
 - 2) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;
 - 3) osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania i nie występują nadrzędne prawnie podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 RODO wobec przetwarzania;
 - 4) dane osobowe były przetwarzane niezgodnie z prawem;
 - 5) dane muszą zostać usunięte w celu wywiązania się z obowiązku prawnego.
- 5th Realizacja „prawa do bycia zapomnianym” następuje przez usunięcie lub anonimizację danych. Jeżeli Administrator upublicznił dane osobowe, a ma obowiązek usunąć te dane, to biorąc pod uwagę dostępną technologię i koszt realizacji podejmuje rozsądne działania, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie kopie i nośniki tych danych osobowych.
- 6th Prawo do ograniczenia przetwarzania – uprawnienie do żądania od Administratora ograniczenia przetwarzania w następujących przypadkach:
 - 1) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający

- Administratorowi sprawdzić prawidłowość tych danych;
- 2) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
 - 3) Administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
 - 4) osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie Administratora są nadrzędne wobec podstaw sprzeciwu.
- 7th Jeżeli przetwarzanie zostało ograniczone, Administrator przetwarza takie dane, za wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby, lub z uwagi na względy interesu publicznego. Przed uchynieniem ograniczenia przetwarzania zgodnie z ust. 2, Administrator informuje o tym osobę, której dane dotyczą, która żądała ograniczenia.
- 8th Prawo do przeniesienia danych do innego administratora – uprawnienie do otrzymania w powszechnie używanym formacie nadającym się do odczytu danych osobowych oraz prawo przesłania danych innemu administratorowi, jeżeli przetwarzanie odbywa się na podstawie zgody w myśl art. 6 ust. 1 lit. a lub art. 9 ust. 2 lub na podstawie umowy w myśl art. 6 ust. 1 lit. b RODO, oraz przetwarzanie odbywa się w sposób zautomatyzowany.
- 9th Wykonując prawo do przenoszenia danych na mocy ust. 1, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez Administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe. Po zgłoszeniu żądania, o którym mowa w ust. 1, Administrator wykona kopię danych osobowych osoby zgłaszającej żądanie znajdujących się w zbiorach Administratora oraz przekaze kopię tych danych na wskazany przez nią adres.
- 10th Prawo do sprzeciwu – uprawnienie do wniesienia sprzeciwu wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e lub f RODO. Po zgłoszeniu sprzeciwu, Administrator nie będzie już przetwarzać tych danych osobowych, chyba że istnieją ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby, której dane dotyczą, lub istnieją podstawy do ustalenia, dochodzenia lub obrony roszczeń. Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych na potrzeby takiego marketingu, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem. Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do marketingu bezpośredniego, danych nie wolno przetwarzać do takich celów.
- 11th Prawo do niepodlegania profilowaniu – uprawnienie do niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowanych przetwarzaniu, w tym profilowaniu i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.

X. Procedura realizacji praw osób, których dane dotyczą

- 1st Realizując prawa osób, których dane dotyczą, Administrator zapewnia gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnicę handlową, dobra osobiste itp.), Administrator może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.
- 2nd Administrator informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.
- 3rd Administrator informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.
- 4th Na żądanie osoby dotyczące dostępu do jej danych, Administrator informuje osobę, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych.
- 5th Na żądanie Administrator wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej

- kopii danych. Administrator wprowadza i utrzymuje cennik kopii danych, zgodnie z którym pobiera opłaty za kolejne kopie danych. Cena kopii danych skalkulowana jest w oparciu o oszacowany jednostkowy koszt obsługi żądania wydania kopii danych.
- 6th Administrator dokonuje sprostowania nieprawidłowych danych na żądanie osoby. Administrator ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.
- 7th Administrator uzupełnia i aktualizuje dane na żądanie osoby. Administrator ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych. Administrator może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Administratora procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.
- 8th Na żądanie osoby, Administrator usuwa dane, gdy:
- 1) dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach;
 - 2) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania;
 - 3) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych;
 - 4) dane były przetwarzane niezgodnie z prawem;
 - 5) konieczność usunięcia wynika z obowiązku prawnego.
- 9th Administrator określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17. ust. 3 RODO. Jeżeli dane podlegające usunięciu zostały upublicznione przez Administratora, Administrator podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, o potrzebie usunięcia danych i dostępu do nich. W przypadku usunięcia danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.
- 10th Administrator dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:
- 1) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość;
 - 2) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
 - 3) nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
 - 4) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Administratora zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu. W trakcie ograniczenia przetwarzania Administrator przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego. Administrator informuje osobę przed uchyleniem ograniczenia przetwarzania. W przypadku ograniczenia przetwarzania danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.
- 11th Na żądanie osoby Administrator wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Administratorowi, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Administratora.
- 12th Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Administratora w oparciu o uzasadniony interes lub o powierzone zadanie w interesie publicznym, Administrator uwzględni sprzeciw, o ile nie zachodzą po stronie Administratora ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.
- 13th Osoba, której dane dotyczą, może złożyć do Administratora wniosek dotyczący skorzystania z praw, które jej przysługują. Wzór wniosku stanowi załącznik nr 8 do niniejszej Polityki.
- 14th Jeśli osoba, której dane dotyczą, złoży wniosek w innej formie niż wskazany w ust. 13 powyżej Administrator jest zobowiązany do jego realizacji.

15th Administrator realizuje żądania osób, których dane dotyczą niezwłocznie, w terminach określonych przepisami prawa.

B. ZASADY DLA UŻYTKOWNIKÓW – ZABEZPIECZENIA FIZYCZNE

XI. Zabezpieczenie dokumentacji papierowej z danymi osobowymi

- 1st Upoważnieni użytkownicy są zobowiązani do stosowania tzw. „polityki czystego biurka”. Polega ona na zabezpieczaniu (zamykaniu) dokumentów w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.
- 2nd Upoważnieni użytkownicy zobowiązani są do bezpiecznego niszczenia dokumentów i wydruków np. w niszczarkach odpowiedniej jakości (niszczarka od poziomu P-4 tak zwana „strzępkowa”).
- 3rd Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. na korytarzach, kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych.
- 4th Zabrania się wyrzucania niezniszczonych dokumentów do śmietnika lub porzucania ich na zewnątrz, np. na terenach publicznych, miejskich lub w lesie.
- 5th Użytkownik przewożący dokumenty jest zobowiązany do ich zabezpieczenia przed zgubieniem, kradzieżą lub innym nieuprawnionym dostępem.
- 6th Zabrania się pozostawiania dokumentów w aucie służbowym/prywatnym podczas nieobecności osoby upoważnionej.
- 7th Wysyłając dokumenty zawierające dane osobowe przy wykorzystaniu Poczty Polskiej należy upewnić się co do prawidłowości adresu odbiorcy oraz stosować wysyłkę rejestrowaną (np. list polecony).
- 8th Wysyłając dokumenty przy wykorzystaniu firm kurierskich należy wykorzystywać wyłącznie firmy sprawdzone, zarejestrowane i działające w oparciu o ustawę prawo przewozowe. Za prawidłowe zabezpieczenie przesyłki pocztowej/kurierskiej odpowiada Administrator zgodnie z obowiązującym regulaminem u danego operatora.
- 9th W przypadku braku stosownego uprawnienia przewidzianego w obowiązujących przepisach prawa, zabrania się tworzenia oraz przechowywania kopii dokumentów publicznych (np. dowodu osobistego, prawa jazdy) pod rygorem odpowiedzialności karnej przewidzianej w ustawie z dnia 22 listopada 2018 r. o dokumentach publicznych.

XII. Polityka kluczy

- 1st Polityka kluczy obejmuje pomieszczenia Administratora.
- 2nd Upoważnienia do pobierania kluczy do pomieszczeń mają wyłącznie osoby wskazane przez Administratora.
- 3rd Klucze do pomieszczeń wydawane i zdawane są za pobraniem z wyznaczonego pomieszczenia.
- 4th Klucze zapasowe przechowywane są w wyznaczonym pomieszczeniu. Wydawanie kluczy zapasowych upoważnionym użytkownikom może odbywać się tylko w uzasadnionych sytuacjach oraz przypadkach awaryjnych za zgodą Administratora. Klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić.
- 5th Klucze służące do zabezpieczenia biurek i szaf muszą być jednoznacznie opisane oraz schowane w miejscu zabezpieczonym.
- 6th W godzinach pracy klucze pozostają pod nadzorem użytkowników, którzy ponoszą za nie pełną odpowiedzialność.
- 7th Zabrania się pozostawiania kluczy w biurkach i szafach podczas chwilowej nieobecności osób upoważnionych w pomieszczeniu.
- 8th Po zakończeniu pracy, klucze służące do zabezpieczenia biurek i szaf muszą być przechowywane w zabezpieczonym miejscu.
- 9th Po zakończeniu pracy, użytkownicy są zobowiązani do zabezpieczenia pomieszczeń a w szczególności wyłączenia i zabezpieczenia urządzeń elektronicznych oraz elektrycznych, wyłączenia oświetlenia, zabezpieczenia i zamknięcia okien i drzwi.
- 10th Naruszenie zasad polityki kluczy może spowodować wyciągnięcie konsekwencji wynikających z art. 52 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy oraz z art. 363 § 1 ustawy z dnia 23 kwietnia 1964 r. Kodeks

cywilny.

11th Dostęp do serwerowni powinien być objęty ścisłym nadzorem tj. Administrator powinien rejestrować każde wejście i wyjście do pomieszczenia.

C. ZASADY DLA UŻYTKOWNIKÓW - IT

XIII. Bezpieczne użytkowanie sprzętu IT, dysków, programów

- 1st W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT, zobowiązany jest do jego ochrony przed jakimkolwiek zniszczeniem lub uszkodzeniem. Za sprzęt IT rozumie się między innymi: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, tablety, smartfony, telefony, karty pamięci, dyski zewnętrzne itp.
- 2nd W przypadku kradzieży, zgubienia, utraty, uszkodzenia lub zniszczenia sprzętu IT, użytkownik powinien natychmiast powiadomić Administratora lub IOD, zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane.
- 3rd Samowolne otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.
- 4th Użytkownik jest zobowiązany do zabezpieczenia sprzętu IT hasłem zgodnie z zasadami opisanymi w rozdziale „Polityka haseł”.
- 5th Sprzęt IT, na którym są dane osobowe, wynoszony poza siedzibę Administratora musi być zaszyfrowany (np. szyfrowane dyski, pliki, itd.).
- 6th W przypadku korzystania ze sprzętu prywatnego do celów służbowych, w szczególności komputery należy utworzyć odrębny od prywatnego profil, do którego dostęp będą mieć wyłącznie osoby upoważnione.
- 7th Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym wglądu do danych wyświetlanych na monitorach komputerowych.
- 8th Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (np. poprzez użycie skrótu WIN+L) lub wylogować się z systemu bądź z programu.
- 9th Po zakończeniu pracy, użytkownik zobowiązany jest:
 - 1) wylogować się z systemu informatycznego, a jeśli to wymagane – następnie wyłączyć sprzęt komputerowy;
 - 2) zabezpieczyć stanowisko pracy, w szczególności wszelkie nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.
- 10th Użytkownik może odstąpić od zasady określonej w ust. 9, tylko na polecenie Administratora np. w przypadku pracy zdalnej.
- 11th Użytkownik jest zobowiązany do usuwania plików z nośników/dysków, do których mają dostęp inni użytkownicy nieupoważnieni do dostępu do takich plików (np. podczas współużytkowania komputerów).
- 12th Użytkownicy komputerów przenośnych, na których znajdują się dane osobowe lub z dostępem do danych osobowych przez Internet zobowiązani są do stosowania zasad bezpieczeństwa.
- 13th Na komputerach przenośnych przeznaczonych do zewnętrznych prezentacji multimedialnych nie powinny, o ile jest to możliwe, znajdować się dane osobowe lub stanowić tajemnicę Administratora.
- 14th Użytkownik zobowiązany jest do zabezpieczenia komputera przenośnego w czasie transportu, a w szczególności:
 - 1) stosowanie szyfrowania dysku twardego komputera;
 - 2) zaleca się przenoszenie go w specjalnym futerale. Dobrym sposobem na zmylenie potencjalnego złodzieja jest przenoszenie komputera przenośnego w zwykłej teczce/aktówce. Sugeruje to przenoszenie dokumentów, a ukrywa fakt transportu komputera przenośnego;
 - 3) zabrania się pozostawiania komputera przenośnego w samochodzie podczas postoju w miejscu publicznym bez nadzoru. Złodzieje dysponują aparaturą umożliwiającą wykrywanie nawet ukrytych komputerów przenośnych;
 - 4) podczas jazdy samochodem zaleca się przechowywanie komputera przenośnego w sposób uniemożliwiający kradzież. Zabrania się przewożenia go np. na siedzeniach, co może skutkować kradzieżą na skrzyżowaniach, przejściach dla pieszych lub w korkach.

- 15thW przypadku, gdy komputer przenośny pozostawiony jest w miejscu dostępnym dla osób nieupoważnionych, użytkownik jest zobowiązany do stosowania kabla zabezpieczającego. W szczególności dotyczy to zabezpieczenia komputera na stanowisku pracy, podczas konferencji, prezentacji, szkoleń, targów itp.
- 16thW przypadku pozostawiania komputerów przenośnych w biurze zaleca się umieszczanie ich po zakończeniu pracy w zamykanych szafkach.
- 17thPracując na komputerze przenośnym w miejscach publicznych i środkach transportu, użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych np. poprzez stosowanie na ekranie filtru prywatyzującego.
- 18thW przypadku korzystania ze sprzętu firmy Apple wykorzystującego między innymi system iOS oraz Mac OS należy:
- 1) wyłączyć automatyczną synchronizację plików z chmurą iCloud,
 - 2) backup urządzenia należy robić po podłączeniu do komputera służbowego, który nie ma włączonej automatycznej synchronizacji plików z chmurą iCloud.
- 19thNie wolno włączać synchronizacji z chmurami, które nie są własnością Administratora (np. zakazana jest synchronizacja telefonu służbowego z prywatnym kontem Google).
- 20thW przypadku braku możliwości wyłączenia automatycznej synchronizacji należy pracować w przeglądarkach internetowych oraz chmurach udostępnionych przez Administratora. Nie należy pobierać plików zawierających dane osobowe do pamięci sprzętu.
- 21st Administrator lub osoba przez niego wyznaczona np. informatyk, zobowiązany jest do monitorowania i analizy logów systemowych oraz aplikacyjnych pod kątem wystąpienia niepożądanych zdarzeń. Zarządzanie i przechowywanie logów powinno być zgodne z Krajowymi Ramami Interoperacyjności.
- 22nd Administrator lub osoba przez niego wyznaczona np. informatyk, zobowiązany jest do bieżącej aktualizacji wszystkich urządzeń IT i systemów informatycznych.

XIV. Korzystanie z usług opartych na sztucznej inteligencji

1. Administrator zanim wyrazi zgodę na korzystanie z usług opartych na sztucznej inteligencji (dalej „usługa”) musi wykonać analizę ryzyka oraz ocenę skutków. Proces ten powinien uwzględniać potencjalne zagrożenia związane z przetwarzaniem danych oraz wpływ zastosowania technologii AI na prawa i wolności osób, których dane dotyczą. Ocena skutków powinna także obejmować zgodność z obowiązującymi przepisami prawa oraz normami etycznymi.
2. Administrator jest zobowiązany do poinformowania IOD o zamiarze korzystania z usług opartych na sztucznej inteligencji. Współpraca z IOD jest kluczowa dla zapewnienia zgodności procesów przetwarzania danych z obowiązującymi regulacjami oraz dla identyfikacji potencjalnych środków zabezpieczających, które mogą minimalizować ryzyko naruszenia ochrony danych osobowych.
3. Przed dopuszczeniem użytkownika do korzystania z zatwierdzonych przez Administratora usług opartych na sztucznej inteligencji użytkownik musi zostać przeszkolony. Program szkoleniowy powinien obejmować zasady bezpiecznego korzystania z technologii AI, świadomość potencjalnych zagrożeń związanych z ochroną danych osobowych oraz najlepsze praktyki w zakresie ich przetwarzania.
4. Administrator zobowiązany jest do bieżącego monitorowania funkcjonowania wdrożonych usług opartych na sztucznej inteligencji oraz przeprowadzania okresowych audytów ich zgodności z przepisami o ochronie danych osobowych. Należy także systematycznie oceniać wpływ technologii na prywatność użytkowników i podejmować stosowne działania korygujące, jeżeli zostaną zidentyfikowane jakiegokolwiek nieprawidłowości.
5. Przed rozpoczęciem korzystania z usług opartych na sztucznej inteligencji np. ChatGPT, należy zapoznać się z dokumentami związanymi z korzystaniem z usługi (np. polityką prywatności).
6. Należy monitorować zmiany w treści polityk, o których mowa w ust. 5 powyżej.
7. Konta w usłudze opartej na sztucznej inteligencji nie powinny być zakładane na imiennych skrzynkach użytkowników.
8. Usługa musi być zgodna z niniejszą Polityką Ochrony Danych Osobowych.
9. Należy zapoznać się z zasadami prawidłowego zadawania pytań, w szczególności jak dostarczać informacji, na podstawie których uzyska się wyniki.
10. Należy przestrzegać poniższych zakazów:
 - 1) nie wolno wprowadzać do usługi danych osobowych, w szczególności: imię, nazwisko, PESEL, stan

zdrowia, sytuacja ekonomiczna, rodzinna, adresy e-mail, życiorys – istnieje realne ryzyko utraty kontroli nad informacjami wprowadzanymi do usługi (Input), to znaczy nie wiadomo, komu te informacje zostaną ujawnione i do czego wykorzystane;

- 2) nie wolno wprowadzać do usługi informacji stanowiących tajemnicę służbową lub tajemnicę zawodową np. dane medyczne, kody źródłowe;
 - 3) nie wolno wprowadzać do usługi takich danych jak Loginy i hasła (np. w celu zbadania siły hasła);
 - 4) nie wolno wklejać pełnych treści dokumentów, które stanowią procedury w zakresie bezpieczeństwa informacji lub danych osobowych np. pełna treść polityki ochrony danych osobowych, analiza ryzyka;
 - 5) nie wolno bez analizy i dokonania sprawdzenia posługiwać się wygenerowaną odpowiedzią – należy pamiętać, że sztuczna inteligencja może posługiwać się nieprawdziwymi informacjami;
 - 6) nie wolno umieszczać dokumentów Administratora, jeśli nie mają statusu publicznego i/lub zawierają dane osobowe.
11. Przykładowe naruszenia/niewłaściwe zachowania w usłudze opartej o sztuczną inteligencję znajdują się w załączniku nr 7.

XV. Wykorzystanie biometrii do zabezpieczenia sprzętu służbowego

1. W przypadku wyrażenia dobrowolnej i świadomej zgody przez użytkownika, dopuszcza się możliwość wykorzystania danych biometrycznych do zabezpieczenia dostępu do sprzętu służbowego.
2. Przetwarzanie danych biometrycznych odbywa się wyłącznie w celu zabezpieczenia sprzętu i nie obejmuje innych procesów przetwarzania.
3. Użytkownik ma prawo w każdej chwili wycofać zgodę na przetwarzanie swoich danych biometrycznych, co skutkuje usunięciem tych danych ze sprzętu służbowego.
4. Po zakończeniu użytkowania sprzętu lub w przypadku jego zwrotu, dane biometryczne są trwale usuwane poprzez sformatowanie urządzenia lub usunięcie kluczy szyfrujących z urządzenia.
5. Administrator zapewnia, że dane biometryczne nie są przechowywane w innych systemach ani nie są wykorzystywane do celów innych niż określone w niniejszej polityce.

XVI. Bezpieczeństwo wymiennych nośników informacji

1st Przez wymienne nośniki informacji rozumie się między innymi: taśmy, pamięci typu flash, pendrive USB, wyjmowane dyski twarde, przenośne dyski twarde USB, płyty CD i DVD, dyktafony.

2nd Użytkownik używając wymiennych nośników informacji bezwzględnie stosuje następujące zasady:

- 1) zabrania się wnoszenia danych osobowych z systemu informatycznego Administratora zapisywanych na wymiennych nośnikach danych poza siedzibę Administratora bez jego zgody;
- 2) w przypadku wnoszenia danych osobowych poza siedzibę Administratora należy wymienne nośniki zaszyfrować, za prawidłowe zabezpieczenie nośników odpowiada Administrator;
- 3) w przypadku braku możliwości zaszyfrowania nośnika danych należy niezwłocznie usuwać dane osobowe po przeniesieniu ich do bezpiecznej infrastruktury IT;
- 4) za nośnik danych i bezpieczeństwo zapisanych na nim danych odpowiada użytkownik;
- 5) wszystkie wymienne nośniki danych, które zawierają dane osobowe z systemu informatycznego Administratora, muszą być przechowywane w miejscach uniemożliwiających do nich dostęp osobom nieupoważnionym w zamykanych szafach lub szafach pancernych;
- 6) na wymiennym nośniku informacji, dane mogą być przechowywane tylko przez czas do tego niezbędny – w przypadku ustania celu przetwarzania danych osobowych zostają niezwłocznie usunięte przez użytkownika;
- 7) wszystkie wymienne nośniki informacji muszą być przechowywane w bezpiecznym środowisku w warunkach zgodnych z wymaganiami producenta. W przypadku, gdy czas życia nośnika (określony przez producenta) jest krótszy od sumarycznego czasu przechowywania informacji, należy dodatkowo zapewnić, aby na skutek pogorszenia się jakości nośnika nie nastąpiła utrata informacji;
- 8) wycofane nośniki informacji, nie mogą być wnoszone poza obszary przetwarzania danych u Administratora bez wcześniejszego skutecznego usunięcia danych.

3rd Uszkodzone wymienne nośniki informacji są niszczone przez upoważnione osoby przez Administratora w sposób uniemożliwiający odczytanie zapisanych na nich danych.

- 4th Wycofanie z eksploatacji wymiennych nośników informacji, przekazanie do naprawy lub ponownego użycia, jest poprzedzone archiwizacją a następnie skutecznym usunięciem zapisanych danych.
- 5th W przypadku zgubienia nośnika z danymi, fakt ten musi zostać zgłoszony do bezpośredniego przełożonego oraz do IOD.
- 6th Zabrania się używania prywatnych zewnętrznych nośników komputerowych lub nośników niewiadomego pochodzenia w infrastrukturze systemów informatycznych Administratora.
- 7th W przypadku konieczności zapisu/odczytu informacji na wymiennym nośniku informacji dostarczonych przez kontrahenta Administratora, użytkownik musi skontaktować się z osobą wyznaczoną np. informatykiem, w celu umożliwienia dostępu do danych znajdujących się na nośniku.
- 8th W sytuacji usuwania danych z dysków twardych oraz innych nośników stosuje się następujące zasady:
- 1) fizyczne usunięcie, to usunięcie danych i informacji, które całkowicie uniemożliwia ich odtworzenie, skasowanie pliku nie wiąże się z fizycznym usunięciem danych lub informacji;
 - 2) usunięcie danych i informacji, to czynność zniszczenia danych i informacji lub taka ich modyfikacja, która nie pozwoli na ponowne odtworzenie danych i informacji;
 - 3) w przypadku nośników przeznaczonych do dalszego użytku w systemie informatycznym Administratora wykonuje się formatowanie;
 - 4) za zniszczenie nośników informacji takich jak płyty CD-R lub CD-RW, DVD, dyskietki, karty procesorowe odpowiada użytkownik wykorzystując odpowiednią do tego niszczarkę (DIN zgodny z typem dokumentów);
 - 5) jeśli nośnik danych (np. pamięć USB, dysk twardy, itp.) zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, to należy go zniszczyć mechanicznie.

XVII. Zarządzanie uprawnieniami

- 1st Każdy użytkownik z dostępem do danych osobowych (np. na komputerze, na dysku sieciowym, w programie lub aplikacji, w poczcie elektronicznej) musi posiadać swój własny indywidualny identyfikator (login) do logowania się.
- 2nd Użytkownik otrzymuje dostęp i odpowiednie uprawnienia do zasobów i aplikacji na polecenie przełożonych i przy realizacji osób odpowiedzialnych za administrowanie systemów.
- 3rd Użytkownicy nie mają prawa do samodzielnej zmiany uprawnień, np. przydzielenia sobie uprawnień administratora.
- 4th Użytkowników obowiązuje zasada pracy na własnym koncie. Zabronione jest zatem umożliwianie innym osobom praca na koncie innego użytkownika.

XVIII. Polityka haseł

- 1st Hasła powinny składać się z min. 14 znaków zawierając małe i duże litery, cyfry i symbole lub powinny się składać z co najmniej 16 znaków zawierając 4-5 losowych wyrazów.
- 2nd Hasła nie mogą być łatwe do odgadnięcia. W szczególności nie należy jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów, typowych zestawów: 123456, qwerty.
- 3rd Hasła nie powinny być ujawnianie innym osobom.
- 4th Nie wolno zapisywać haseł na kartkach i w notesach, naklejać na monitorze komputera, trzymać pod klawiaturą lub w szufladzie.
- 5th Nie wolno zapisywać haseł w przeglądarce internetowej, jeśli nie zawiera ona odpowiednich zabezpieczeń np. dwuetapowej metody uwierzytelniania. Za weryfikację odpowiednich zabezpieczeń odpowiada Administrator.
- 6th Za zgodą Administratora można dopuścić do stosowania szyfrowane menadżery haseł np. KeePass.
- 7th W przypadku ujawnienia hasła – należy natychmiast je zmienić, a fakt ujawnienia zgłosić Administratorowi i Inspektorowi Ochrony Danych.
- 8th Hasła powinny być zmieniane co 90 dni. Decyzję o zmianie tego okresu może podjąć Administrator biorąc pod uwagę między innymi złożoność stosowanych haseł. Jeśli hasło zostaje zmienione musi być zupełnie inne niż poprzednie.

- 9th Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła.
- 10th Zmiana hasła polega na utworzeniu całkowicie nowego hasła, innego niż co najmniej 8 poprzednich haseł.
- 11th W przypadku przetwarzania danych we własnych systemach informatycznych (m.in. adresach e-mailowych w wykupionej domenie, stronach internetowych, aplikacjach) należy stosować uwierzytelnianie co najmniej dwustopniowe (np. podanie loginu oraz hasła + hasła wysłanego wiadomością na podany wcześniej numer telefonu/adres e-mail).
- 12th Jeśli zastosowana zostanie metoda uwierzytelniania dwustopniowego przy logowaniu to zmiana hasła, określona w ust. 8, nie jest wymagana.

XIX. Korzystanie z Internetu

- 1st Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
- 2nd Zabrania się zgrywania na sprzęt IT oraz uruchamiania jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą Administratora lub osoby upoważnionej do administrowania infrastrukturą IT i tylko w uzasadnionych przypadkach.
- 3rd Użytkownik ponosi odpowiedzialność za szkody spowodowane przez nieautoryzowane oprogramowanie instalowane z Internetu.
- 4th Bez zgody Administratora zabrania się:
- 1) wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pomograficznym lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera);
 - 2) logowania na prywatne konta między innymi pocztą e-mail, portale społecznościowe. Ten zakaz nie obowiązuje jeśli Administrator wyda pisemną zgodę na logowanie do tego typu serwisów.
- 5th W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą "https:". Dla pewności należy „kliknąć” na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.
- 6th Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty e-mailowej) lub podania loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie dotyczy to żądania podania takich informacji przez rzekomy bank.
- 7th Należy zweryfikować poprawność adresu strony internetowej, na której podawane będą dane uwierzytelniające lub dane osobowe.
- 8th Zabrania się korzystania z publicznych sieci WiFi, a w przypadku niepublicznych sieci dopuszcza się korzystanie tylko w sytuacji, gdy są odpowiednio zabezpieczone. Rekomendowane jest udostępnianie WiFi z telefonu służbowego.

XX. Korzystanie z poczty elektronicznej

- 1st Przesyłanie danych osobowych z użyciem e-maila poza strukturę Administratora może odbywać się tylko przez osoby do tego upoważnione.
- 2nd W przypadku przesyłania danych osobowych poza strukturę Administratora należy wykorzystywać mechanizmy kryptograficzne (szyfrowanie wysyłanych dokumentów lub plików zzipowanych, podpis elektroniczny).
- 3rd W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 10 znaków: litery i cyfry, znak specjalny, a hasło należy przesłać odrębnym środkiem komunikacji lub inną metodą, np. telefonicznie lub SMS-em.
- 4th Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
- 5th Nie wolno otwierać załączników (plików) w e-mailach nawet od rzekomo znanych nam nadawców bez weryfikacji tegoż nadawcy. Tego typu e-maile większości przypadków zawierają załączniki ze szkodliwymi programami, które po „kliknięciu” infekują komputer użytkownika oraz często pozostałe komputery w sieci. W wyniku działania takiego szkodliwego oprogramowania może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowaniem przez kryptowirusy.
- 6th Bez weryfikacji wiarygodności nadawcy, nie wolno „klikać” na hiperlinki w e-mailach, gdyż mogą to być

- hiperlinki do stron zainfekowanych lub niebezpiecznych. Użytkownik „klikając” na taki hiperlink bezwiednie infekuje swój komputer oraz często pozostałe komputery w sieci. W wyniku takiej infekcji może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowaniem przez kryptowirusy.
- 7th Należy zgłaszać Administratorowi przypadki podejrzanych e-maili.
- 8th Użytkownicy nie powinni rozsyłać „niezawodowych” e-maili w formie „łańcuszków szczęścia”, np. życzenia świąteczne adresowane do 230 osób.
- 9th Podczas wysyłania e-maili do wielu adresatów jednocześnie, należy użyć metody „ukryte do wiadomości – „UDW”. Zabronione jest rozsyłanie e-maili do wielu adresatów z użyciem opcji „do wiadomości”. Nie dotyczy to sytuacji, gdy wszyscy adresaci wiadomości ze sobą współpracują w ramach prowadzonych działań.
- 10th Użytkownicy powinni okresowo kasować niepotrzebne e-maile, zgodnie z zasadami dotyczącymi okresu przechowywania danych osobowych obowiązującymi u Administratora.
- 11th Każda osoba, która przetwarza dane osobowe w imieniu Administratora, wykorzystuje w tym celu jedynie e-mail służbowy.
- 12th E-mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.
- 13th Zakazane jest wysyłanie korespondencji służbowej na prywatne skrzynki pocztowe użytkowników lub innych osób lub łączenia poczty służbowej z pocztą prywatną np. poprzez przekierowanie wiadomości e-mail.
- 14th Przy korzystaniu z e-maila, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
- 15th Użytkownicy nie mają prawa korzystać z e-maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.
- 16th Użytkownik bez zgody Administratora nie ma prawa wysłać wiadomości zawierających dane osobowe dotyczące Administratora, jego użytkowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.
- 17th W przypadku wysłania wiadomości e-mail do niewłaściwego odbiorcy należy bezzwłocznie poinformować Administratora lub IOD o takim zdarzeniu, podając jak najbardziej szczegółowy opis zdarzenia. Ponadto, informacja powinna zostać przekazana do bezpośredniego przełożonego użytkownika, który dopuścił się naruszenia. Jeśli incydent skutkuje wysokim prawdopodobieństwem naruszenia praw i wolności osób, których dane dotyczą, Administrator zgłasza go do Prezesa Urzędu Ochrony Danych Osobowych.

XXI. Ochrona antywirusowa

- 1st Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym, jeśli system antywirusowy taką funkcję posiada.
- 2nd Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.
- 3rd W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów np. „Twój system jest zainfekowany!”, zainstaluj program antywirusowy”, użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Administratora. Administrator obowiązany jest na bieżąco sprawdzać i aktualizować ochronę antywirusową na wszystkich urządzeniach służbowych.
- 4th Baza wirusów w programie antywirusowym musi być na bieżąco aktualizowana.

D. ZASADY DLA ADMINISTRATORA – IT

XXII. Wykonywanie przeglądów, konserwacji, napraw sprzętu IT, systemów służących do przetwarzania danych osobowych

- 1st Przeglądy, konserwacja, naprawy baz danych, oprogramowania, sprzętu IT przeprowadzana jest przez Administratora lub osobę upoważnioną. Dopuszczalne jest zaangażowanie firmy zewnętrznej.
- 2nd W przypadku wykonywania przez firmę zewnętrzną jakichkolwiek czynności w systemach lub na sprzęcie IT, na którym znajdują się dane osobowe, należy stosować poniższe zasady bezpieczeństwa:
- 1) czynności wykonywane są na miejscu pod nadzorem Administratora lub osoby upoważnionej;
 - 2) należy zdemonstrować dyski i zabezpieczyć je u Administratora (np. na czas naprawy);
 - 3) należy zgrać dane na inny nośnik i usunąć je z przekazywanego sprzętu.

- 3rd Jeśli firma zewnętrzna dokonująca przeglądu, konserwacji, naprawy oprogramowania, sprzętu IT otrzymuje dostęp do danych osobowych należy zawrzeć umowę powierzenia.
- 4th W przypadku przekazania komputerów innemu użytkownikowi lub jednostce organizacyjnej, dane z dysków twardych są usuwane przez Administratora lub osobę upoważnioną w sposób uniemożliwiający ich odtworzenie.
- 5th W przypadku złomowania sprzętu komputerowego, nośniki informacji (dyski twarde) są fizycznie niszczone przez Administratora lub osobę upoważnioną.
- 6th Informatyk lub osoba wskazana przez Administratora zobowiązana jest do zinwentaryzowania sprzętu służącego do przetwarzania danych osobowych. Rejestr prowadzony w formie elektronicznej lub papierowej zgodnie ze wzorem określonym w załączniku nr 14.
- 7th Informatyk lub osoba wskazana przez Administratora jest zobowiązana do aktualizacji rejestru, o którym mowa w pkt. powyżej, raz do roku.

XXIII. Tworzenie kopii zapasowych

- 1st Kopie zapasowe są wykonywane zgodnie z zasadą 3-2-1-1 tj. na macierze sieciowe 2 odrębne urządzenia oraz dysk przenośny.
- 2nd Kopie zapasowe należy przechowywać na co najmniej dwóch różnych nośnikach, w tym jedną z nich w wersji offline (np. na płycie CD).
- 3rd Kopie zapasowe na serwerze tworzone są w sposób zautomatyzowany w oparciu o wykorzystanie programowej funkcji serwera dostarczonej przez dostawcę systemu.
- 4th W sytuacji przechowywania danych osobowych na dyskach chmurowych np. OneDrive, Google Drive należy określić kluczowe zasoby, z których należy sporządzać kopie zapasowe.
- 5th Kopie całościowe sporządzane są zgodnie z przyjętym harmonogramem zatwierdzonym przez Administratora.
- 6th Kopie sporządzane są na: dyskach zewnętrznych lub płycie DVD/CD lub na serwerach zewnętrznych/wewnętrznych lub taśmach LTO.
- 7th Każdy nośnik jest opisany datą jej sporządzenia.
- 8th Kopie zapasowe przechowywane są tak długo jak wymagają tego przepisy prawa i przyjęty harmonogram, o którym mowa w ust. 1.
- 9th Dostęp do kopii mają osoby upoważnione przez Administratora.
- 10th Kopie przechowywane są miejscu zabezpieczonym na terenie siedziby Administratora lub w miejscu zarządzanym przez Administratora (np. serwer w chmurze).
- 11th Kopie zapasowe powinny być zaszyfrowane, jeśli to możliwe.
- 12th Wykonane kopie zapasowe podlegają testowaniu, mierzeniu i ocenianiu nie rzadziej niż raz na 3 miesiące. Protokół potwierdzający wykonanie czynności sporządza i przechowuje informatyk.

XXIV. Zarządzanie zmianą w systemie, który jest własnością Administratora (usługa własna)

- 1st Administrator przed wprowadzeniem i nie rzadziej niż raz w roku ma obowiązek testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych (nadzór i monitorowanie prac rozwojowych nad systemami,) mających zapewnić bezpieczeństwo przetwarzanych danych osobowych w systemach informatycznych.
- 2nd Administrator odpowiada za określenie poziomów wprowadzanych zmian od kluczowych, które mają znaczący wpływ na bezpieczeństwo danych osobowych po takie, które na bezpieczeństwo mają znikomy wpływ.
- 3rd Zmiana w systemie powinna zostać w sposób formalny zainicjowana u Administratora.
- 4th Komórka organizacyjna odpowiedzialna za wdrażanie zmian przygotowuje oraz w jasny i czytelny sposób przedstawia plan zmian w systemie, w szczególności obszarów, które mogą mieć wpływ na bezpieczeństwo danych osobowych. Plan zatwierdza Administrator.
- 5th W przypadku zmian, które w sposób znaczący mają wpływa na bezpieczeństwo danych osobowych należy uzyskać opinię IOD.
- 6th Za bezpieczne wdrożenie zmian odpowiada wskazana przez Administratora komórka organizacyjna.

7th Testowanie zmian – należy sprawdzić, czy wszystkie problemy systemowe zostały rozwiązane, a zmiany wprowadzone w sposób bezpieczny.

8th Testowanie systemów może odbyć się wyłącznie w środowisku testowym, tj. poza pracą bieżącą systemów.

9th Zabrania się stosowania danych rzeczywistych w charakterze danych testowych.

10th Administrator ma obowiązek:

- 1) ewidencjonowania zmian wprowadzanych w systemach wspomagania zarządzania projektami i ich kontroli;
- 2) stosować zasadę prywatności w fazie projektowania oraz zasadę domyślnej ochrony danych;
- 3) stosować ochronę danych osobowych na etapie projektowania zmian w systemie;
- 4) przeprowadzania regularnych przeglądów bezpieczeństwa danych osobowych w systemie, nie rzadziej niż raz w roku;
- 5) przechowywania dokumentacji dowodowej z przeprowadzanych audytów zabezpieczeń oraz środków technicznych i organizacyjnych.

11th Administrator przy dokonywaniu oceny proporcjonalności zabezpieczeń powinien wziąć pod uwagę czynniki i okoliczności dotyczące przetwarzania (np. rodzaj, sposób przetwarzania danych) i ryzyko, jakie się z nim wiąże.

12th Administrator powinien stosować audyty zabezpieczeń systemów, w których przetwarzane są dane osobowe oraz środków technicznych i organizacyjnych jako najistotniejsze środki bezpieczeństwa. Konieczne jest zapewnienie regularnego monitoringu stosowanych zabezpieczeń.

XXV. Zarządzanie zmianą w systemie, który jest własnością Administratora (Administrator korzysta ze wsparcia podmiotu zewnętrznego – wdrażanie i koordynacja systemu – podmiot przetwarzający)

1st Obowiązki Administratora w stosunku do podmiotu przetwarzającego opisane zostały w rozdziale „Udostępnianie i powierzanie danych osobowych”.

2nd Administrator w umowie powierzenia przetwarzania danych osobowych z podmiotem przetwarzającym zawiera obowiązek stosowania przed wprowadzeniem i nie rzadziej niż raz w roku testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych (nadzór i monitorowanie prac rozwojowych nad systemami) mających zapewnić bezpieczeństwo przetwarzanych danych osobowych w systemach informatycznych oraz przedstawiać nie rzadziej niż raz w roku Administratorowi raporty z prowadzonych testów, itp.

3rd Administrator odpowiada za określenie poziomów wprowadzanych zmian od kluczowych, które mają znaczący wpływ na bezpieczeństwo danych osobowych po takie, które na bezpieczeństwo mają znikomy wpływ.

4th Zmiana w systemie powinna zostać w sposób formalny (np. poprzez pisemne powiadomienie o konieczności wprowadzenia zmiany) zainicjowana przez Administratora lub podmiot zajmujący się koordynacją funkcjonowaniem systemu – podmiot przetwarzający.

5th Komórka organizacyjna odpowiedzialna za wdrażanie zmian przygotowuje oraz w jasny i czytelny sposób przedstawia plan zmian w systemie, w szczególności obszarów, które mogą mieć wpływ na bezpieczeństwo danych osobowych. Plan zatwierdza Administrator.

6th W przypadku zmian, które w sposób znaczący mają wpływa na bezpieczeństwo danych osobowych należy uzyskać opinię IOD.

7th Implementacja zmian – podmiot przetwarzający przeprowadza, a Administrator nadzoruje bezpieczne wdrożenie oraz integrację zmian i procesów w systemie.

8th Administrator i podmiot przetwarzający odpowiadają za testowanie zmian, w szczególności za sprawdzenie bezpieczeństwa systemu i czy wszystkie problemy systemowe zostały rozwiązane.

9th Testowanie systemów może odbyć się wyłącznie w środowisku testowym, tj. poza pracą bieżącą systemów.

10th Zabrania się stosowania danych rzeczywistych w charakterze danych testowych.

11th Administrator i podmiot przetwarzający ma obowiązek ewidencjonowania zmian wprowadzanych w systemach, wspomagania zarządzania projektami i ich kontroli.

13th Administrator ma obowiązek:

- 1) ewidencjonowania zmian wprowadzanych w systemach wspomagania zarządzania projektami i ich kontroli;
 - 2) stosować zasadę prywatności w fazie projektowania oraz zasadę domyślnej ochrony danych;
 - 3) stosować ochronę danych osobowych na etapie projektowania zmian w systemie;
 - 4) przeprowadzania regularnych przeglądów bezpieczeństwa danych osobowych w systemie, nie rzadziej niż raz w roku;
 - 5) przechowywania dokumentacji dowodowej z przeprowadzanych audytów zabezpieczeń oraz środków technicznych i organizacyjnych.
- 14th Administrator i podmiot przetwarzający przy dokonywaniu oceny proporcjonalności zabezpieczeń powinien wziąć pod uwagę czynniki i okoliczności dotyczące przetwarzania (np. rodzaj, sposób przetwarzania danych) i ryzyko, jakie się z nim wiąże.

XXVI. Zarządzenie zmianą w systemie, który nie jest własnością Administratora (Administrator korzysta ze wsparcia podmiotu – podmiot przetwarzający)

- 1st Obowiązki Administratora w stosunku do podmiotu przetwarzającego opisane zostały w rozdziale „Udostępnianie i powierzanie danych osobowych”.
- 2nd Administrator w umowie powierzenia przetwarzania danych osobowych z podmiotem przetwarzającym zawiera obowiązek stosowania przed wprowadzeniem i nie rzadziej niż raz w roku testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych (nadzór i monitorowanie prac rozwojowych nad systemami) mających zapewnić bezpieczeństwo przetwarzanych danych osobowych w systemach informatycznych oraz przedstawiać nie rzadziej niż raz w roku Administratorowi raporty z prowadzonych testów, itp.
- 3rd Administrator powinien dążyć do zawarcia umowy, w której zawarte będą procedury dotyczące zarządzania zmianą.

XXVII. Monitoring wizyjny

- 1st Administrator musi na swoim terenie poinformować o monitoringu, poprzez zamieszczenie wyraźnej informacji na drzwiach, korytarzach, płotach itp.
- 2nd Tablice informujące o zainstalowanym monitoringu powinny być widoczne, syntetyczne, umieszczone w sposób trwały w niezbyt dużej odległości od nadzorowanych miejsc, zaś wymiary tablic muszą być proporcjonalne do miejsca, gdzie zostały umieszczone. Stosowane mogą być dodatkowo piktogramy informujące o objęciu dozorem kamer. Nie jest wystarczające oznaczenie obszaru objętego monitoringiem jedynie piktogramami.
- 3rd W przypadku stosowania wideodomofonu należy umieścić informację, że następuje monitoring w czasie rzeczywistym np. w zakresie wizji i dźwięku.
- 4th Należy zastosować obowiązek informacyjny, o którym mowa w rozdziale „Obowiązek informacyjny i wyrażenie zgody”, ale nie trzeba wywieszać go w każdym miejscu monitorowania. Obowiązek ten musi znajdować się miejscu widocznym przy wejściu na teren objęty monitoringiem.
- 5th Prawa osób objętych monitoringiem obejmują m.in.:
- 1) prawo do informacji o istnieniu monitoringu w określonym miejscu, jego zasięgu, celu, nazwie podmiotu odpowiedzialnego za instalację, jego adresie i danych do kontaktu;
 - 2) prawo dostępu do nagrań w uzasadnionych przypadkach;
 - 3) prawo żądania usunięcia danych jej dotyczących;
 - 4) prawo do anonimizacji wizerunku na zarejestrowanych obrazach i/lub usunięcia dotyczących jej danych osobowych;
 - 5) prawo do przetwarzania danych przez ograniczony czas.
- 6th Okres przechowywania danych po dokonaniu nagrania nie może być dłuższy niż 30 dni. W przypadku, w którym nagrania obrazu stanowią dowód w postępowaniu prowadzonym na podstawie prawa lub pracodawca powziął wiadomość, iż mogą one stanowić dowód w postępowaniu, termin ten ulega przedłużeniu do czasu prawomocnego zakończenia postępowania. Po upływie tych okresów uzyskane w wyniku monitoringu nagrania obrazu zawierające dane osobowe podlegają zniszczeniu.

- 7th Do ekranu, na którym odtwarzany jest monitoring mają dostęp tylko osoby upoważnione przez Administratora.
- 8th Rejestrator monitoringu jest obowiązkowo przechowywany w miejscu zamkniętym dla osób trzecich, a dostęp do niego mają tylko osoby upoważnione przez Administratora. Dostęp do pomieszczenia powinien być rejestrowany.
- 9th W przypadku wykorzystywania monitoringu do celów innych niż zapewnienie bezpieczeństwa, Administrator nie jest uprawniony do przetwarzania pochodzących z niego danych osobowych nawet na podstawie uzyskania wcześniejszych zgód od osób, które miały być nim objęte, gdyż nie jest możliwe, aby zebrać zgodę od wszystkich osób zarejestrowanych na nagraniach. Nie dotyczy to przypadku, kiedy wejście na monitorowany teren jest ograniczone w takim stopniu, że Administrator jest w stanie zebrać zgodę od każdej osoby, która pojawi się na nagraniu.
- 10th Stosowanie monitoringu dozwolone jest w celu: zapewnienia bezpieczeństwa, ochrony mienia, kontroli produkcji, zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę.
- 11th Monitoringu nie można stosować w celu: nadzoru nad jakością wykonywania pracy.
- 12th Niedozwolone jest instalowanie atrap kamer monitoringu.
- 13th Podejmując decyzję o wprowadzeniu monitoringu, Administrator musi przeprowadzić ocenę skutków dla ochrony danych. Jest ona wymagana, gdy operacja przetwarzania ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych (np. w przypadku systematycznego monitorowania miejsc publicznych). Ocena zawiera:
- 1) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez Administratora;
 - 2) ocenę czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
 - 3) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
 - 4) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

E. ZASADY DLA ADMINISTRATORA – OGÓLNE

XXVIII. Projektowanie prywatności

Administrator zarządza zmianą mającą wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania. W tym celu zasady prowadzenia projektów i inwestycji przez Administratora odwołują się do zasad bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę danych, uwzględnienia i zaprojektowania bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub inwestycji.

XXIX. Identyfikacja obszarów wymagających szczególnych zabezpieczeń

Uwzględniając kategorie przetwarzanych danych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka, stosuje się wysoki poziom bezpieczeństwa. Administrator akceptuje poziom ryzyka oszacowany w rejestrze czynności przetwarzania, opracowany na podstawie „Analizy zagrożeń i ryzyka”. IOD przeprowadza okresową (nie rzadziej niż raz na rok) analizę ryzyka dla poszczególnych systemów i na tej podstawie przedstawia Administratorowi propozycje dotyczące zastosowania środków technicznych i organizacyjnych, celem zapewnienia właściwej ochrony przetwarzanym danym.

XXX. Analiza zagrożeń i ryzyka

1. Administrator przeprowadza w trybie bieżącym analizę zagrożeń i ryzyka, której celem jest ocena ryzyka, czyli określenie, które ryzyka są akceptowalne poprzez porównanie wyznaczonych poziomów ryzyka z tymi, które można akceptować.
2. Metodologia oraz wzór analizy zagrożeń i ryzyka stanowią załącznik nr 12.
3. Analiza ryzyka prowadzona jest w rejestrze czynności przetwarzania danych osobowych.

XXXI. Ocena skutków dla ochrony danych (DPiA)

1. Administrator przeprowadza ocenę skutków dla ochrony danych (dalej DPiA), gdy przetwarzanie danych osobowych wiąże się z ryzykiem lub wysokim ryzykiem naruszenia praw osób, których dane dotyczą.
2. DPiA realizuje się przed przystąpieniem do przetwarzania danych osobowych (na etapie planowania).
3. DPiA stosuje się w szczególności, gdy:
 - 1) dokonuje się systematycznej, kompleksowej, zautomatyzowanej oceny czynników osobowych, na podstawie, której podejmowane są decyzje wywołujące skutki prawne wobec osoby fizycznej;
 - 2) przetwarza się na dużą skalę dane osobowe szczególnej kategorii;
 - 3) systematycznie monitoruje się na dużą skalę miejsca dostępne publicznie.
4. Ocenę przeprowadza się w porozumieniu z IOD oraz na wzorze przez niego dostarczonym.

XXXII. Testowanie środków technicznych i organizacyjnych

- 1st Testy środków technicznych i organizacyjnych powinny odbywać się w regularnych odstępach czasu minimum raz w roku lub po każdej istotnej zmianie w procedurach lub innych aktywach.
- 2nd Za wykonanie testów, o których mowa w ust. 1 powyżej odpowiada Administrator Danych Osobowych lub osoba/osoby przez niego upoważnione.
- 3rd Wyniki testów należy dokumentować np. poprzez sporządzenie raportu, podsumowania, notatki służbowej, oświadczeń.
- 4th Wyniki z wykonanych testów powinny być przekazane IOD.
- 5th Wykaz przykładowych działań z zakresu testowania środków technicznych i organizacyjnych stanowi załącznik nr 11.

F. NARUSZENIA OCHRONY DANYCH OSOBOWYCH

XXXIII. Postępowanie na wypadek wystąpienia naruszenia ochrony danych

- 1st Procedura została opracowana w celu zapewnienia sprawnego oraz prawidłowego reagowania na wystąpienie naruszenia ochrony danych osobowych. Ma ona zastosowanie do wszelkich danych osobowych przetwarzanych przez Administratora zarówno w jego siedzibie, jak i poza nią.
- 2nd Katalog przykładowych zagrożeń i naruszeń, jakie mogą wystąpić w związku z przetwarzaniem danych znajduje się w załączniku nr 7 do niniejszej Polityki.
- 3rd Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia Administratora bądź osób przez niego upoważnionych o przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych. Zawiadomienie ma nastąpić bez zbędnej zwłoki, ale w przeciągu 18 godzin od zaistnienia sytuacji. Osoba stwierdzająca naruszenie musi uzupełnić raport, który stanowi załącznik nr 5 do niniejszej Polityki.
- 4th Osoba, która stwierdzi fakt naruszenia ma obowiązek podjąć działania niezbędne do powstrzymania skutków naruszenia oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn i skutków naruszenia.
- 5th Administrator podejmuje działania w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w celu zminimalizowania jego ewentualnych negatywnych skutków.
- 6th Administrator przeprowadza analizę pod kątem wystąpienia ryzyka naruszenia praw i wolności osób fizycznych. W przypadku stwierdzenia:
 - 1) braku lub niskiego prawdopodobieństwa wystąpienia ryzyka Administrator zwolniony jest z obowiązku powiadamiania Prezesa UODO oraz osoby, której dane dotyczą o naruszeniu. Wnioski z przeprowadzonej analizy należy odnotować w wewnętrznym rejestrze naruszeń;
 - 2) wysokiego prawdopodobieństwa wystąpienia ryzyka Administrator ma obowiązek:
 - a) bez zbędnej zwłoki zawiadomić osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych zgodnie z zasadą przejrzystości. Należy uważać, aby nie wykorzystywać kanału kontaktowego, który w wyniku naruszenia przestał być bezpieczny. Zasadą jest powiadamianie bezpośrednie (np. e-mail, SMS), natomiast gdy wymagałoby to niewspółmiernie dużego wysiłku Administrator powiadamia o naruszeniu komunikatem publicznym lub podobnym środkiem, za pomocą którego osoby, których dane dotyczą, zostaną poinformowane o naruszeniu w równie skuteczny sposób;
 - b) bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, zawiadomić

organ nadzorczy (Prezesa UODO). W przypadku nieposiadania przez Administratora w terminie wyznaczonym do udzielenia zgłoszenia wszystkich wymaganych informacji dotyczących naruszenia, zgłoszenie należy sukcesywnie uzupełniać podając przyczyny opóźnienia.

7th Naruszenia związane z atakami phishingowymi Administrator zgłasza również przez stronę www.incydent.cert.pl.

8th Administrator w związku z podleganiem pod ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa musi zgłaszać naruszenia cyberbezpieczeństwa w ciągu 24 godzin od stwierdzenia podejrzenia naruszenia przez stronę www.incydent.cert.pl.

XXXIV. Analiza wystąpienia ryzyka naruszenia praw i wolności osób fizycznych

1st Administrator „stwierdza” naruszenie, kiedy ma on wystarczający stopień pewności co do tego, że miało miejsce zdarzenie zagrażające bezpieczeństwu, które doprowadziło do naruszenia ochrony danych.

2nd Konsekwencją stwierdzenia naruszenia jest konieczność przeprowadzenia analizy pod kątem ryzyka naruszenia praw lub wolności osób, których dane dotyczą – od tego zależy czy naruszenie będzie podlegało zgłoszeniu do Prezesa UODO.

3rd Administrator dokonuje analizy każdorazowo w odniesieniu do konkretnego naruszenia.

4th W ocenie ryzyka naruszenia praw i wolności osób fizycznych konieczne jest uwzględnienie:

- 1) powagi zdarzenia tj. wielkości szkody, jakie zdarzenie to może spowodować w odniesieniu do osoby, której dane dotyczą;
- 2) prawdopodobieństwa wystąpienia tego zdarzenia będącego skutkiem naruszenia.

5th Stopień dotkliwości w przypadku zmaterializowania się zagrożenia należy oceniać z perspektywy osób, których dane są przetwarzane.

6th Dla poziomu potencjalnego ryzyka może mieć znaczenie fakt posiadania przez Administratora wiedzy, że dane osobowe znajdują się w rękach osób, których zamiary są nieznane lub które mogą mieć złe intencje.

7th Nie jest konieczne, aby ryzyko się zmaterializowało (by faktycznie doszło do naruszenia). Należy ocenić prawdopodobieństwo zaistnienia szkody w przypadku danego zdarzenia.

8th W przypadku jakichkolwiek wątpliwości Administrator powinien zgłosić naruszenie, nawet jeśli taka ostrożność mogłaby się okazać nadmierna.

9th Ryzyko naruszenia praw lub wolności osób fizycznych powstaje, kiedy naruszenie może skutkować fizyczną, materialną lub niematerialną szkodą dla osób fizycznych, których dane naruszono. Szkodami takimi są np.:

- 1) dyskryminacja;
- 2) kradzież tożsamości lub oszustwo dotyczące tożsamości;
- 3) nadużycia finansowe;
- 4) straty finansowe;
- 5) nieuprawnione cofnięcie pseudonimizacji;
- 6) utrata poufności danych osobowych chronionych tajemnicą zawodową;
- 7) naruszenie dobrego imienia;
- 8) lub inne znaczące skutki gospodarcze lub społeczne dla danej osoby fizycznej.

1. Jeżeli naruszenie dotyczy danych osobowych ujawniających:

- 1) pochodzenie etniczne;
- 2) poglądy polityczne,
- 3) przekonania religijne lub światopoglądowe;
- 4) przynależność do związków zawodowych;
- 5) dane genetyczne;
- 6) dane dotyczące zdrowia;
- 7) dane dotyczące życia seksualnego;
- 8) dane dotyczące wyroków skazujących lub naruszeń prawa

należy uznać, że występuje duże prawdopodobieństwo takiej szkody. Niemniej jednak każde z takich zdarzeń należy rozpatrywać indywidualnie.

11th Kryteria oceny ryzyka dla osób fizycznych będącego wynikiem naruszenia:

- 1) rodzaj naruszenia;
- 2) charakter, wrażliwość i ilość danych osobowych;

- 3) łatwość identyfikacji osób fizycznych;
- 4) waga konsekwencji dla osób fizycznych;
- 5) cechy szczególne danej osoby fizycznej;
- 6) cechy szczególne Administratora danych;
- 7) liczba osób fizycznych, na które naruszenie wywiera wpływ.

12th Głównymi kryteriami branymi pod uwagę przy ocenie dotkliwości naruszenia danych osobowych są:

- 1) kontekst przetwarzania danych (KPD) – określa typ naruszonych danych wraz z liczbą czynników związanych z ogólnym kontekstem przetwarzania;
- 2) łatwość identyfikacji (LI) – określa jak łatwo można wywnioskować tożsamość osób z danych związanych z naruszeniem;
- 3) okoliczności naruszenia (ON) – określają szczególne okoliczności naruszenia, które są związane z rodzajem naruszenia, w tym głównie z utratą bezpieczeństwa naruszonych danych, jak również wszelkie złośliwe zamiary.

13th Aby zdefiniować wynik dla kontekstu przetwarzania, Administrator danych powinien wykonać następujące kroki:

- 1) określić rodzaje danych osobowych, których dotyczyło naruszenie;
- 2) sklasyfikować dane w co najmniej jednej z czterech kategorii: dane podstawowe, dane szczególnej kategorii, dane finansowe, dane behawioralne (związane z nawykami). W ten sposób otrzymujemy podstawowy wynik KPD;
- 3) punktacja – wynik podstawowy:
 - a) dane podstawowe – 1 pkt.,
 - b) dane behawioralne – 2 pkt.,
 - c) dane finansowe – 3 pkt.,
 - d) dane szczególnej kategorii – 4 pkt.
- 4) Ocenic występowanie czynników bądź zakresów danych, które zwiększają lub zmniejszają wynik podstawowy.

14th Łatwość identyfikacji ocenia jak łatwo będzie dla strony, która ma dostęp do zestawu danych, jednoznacznie dopasować je do określonej osoby. Wyróżniamy cztery poziomy LI: znikome (0,25 pkt.), ograniczone (0,5 pkt.), znaczące (0,75 pkt.) i maksymalne (1,0 pkt.).

15th Przy określaniu okoliczności naruszenia należy brać pod uwagę utratę poufności, integralności i dostępności danych oraz złośliwe zamiary, które uzupełniają KPD i LI w następujący sposób:

- 1) utrata poufności następuje, gdy strony uzyskują dostęp do informacji, do których nie są upoważnione. Stopień utraty poufności zależy od zakresu ujawnienia, tj. potencjalnej liczby i rodzaju stron, które mogą mieć bezprawną dostęp do informacji;
- 2) utrata integralności występuje, gdy oryginalna informacja jest zmieniona i zastąpiona, a zmienione informacje mogą być szkodliwe dla jednostki;
- 3) utrata dostępności następuje, gdy nie można uzyskać dostępu do oryginalnych danych. Sytuacja może być czasowa lub trwała;
- 4) złośliwy zamiar, to element, który określa, czy naruszenie było spowodowane błędem czy też działaniem zamierzonym. Obejmuje to przypadki kradzieży i włamań, jak również przekazywanie danych osobowych osobom trzecim w celu osiągnięcia zysku. Złośliwe intencje to czynnik, który zwiększa prawdopodobieństwo, że dane są wykorzystane w szkodliwy sposób dla jednostki. W zależności od rodzaju okoliczności naruszenia przyznajemy wartości 0, 0,25 lub 0,5.

16th Końcowy wynik oceny dotkliwości naruszenia oblicza się wzorem: (DN): $DN = KPD \times LI + ON$. Wyliczony wynik:

- 1) niski: $DN < 2$;
- 2) średni: $2 \leq DN < 3$;
- 3) wysoki: $3 \leq DN < 4$;
- 4) bardzo wysoki: $4 \leq DN$

należy odnotować w rejestrze naruszeń, który stanowi załącznik nr 4 do niniejszej Polityki.

G. PRZEKAZYWANIE DANYCH OSOBOWYCH

XXXV. Udostępnianie i powierzanie danych osobowych

- 1st Dane osobowe mogą być udostępnione osobom i podmiotom z mocy przepisów prawa lub jeżeli w sposób wiarygodny uzasadnią one potrzebę ich posiadania, a ich udostępnienie nie naruszy praw i wolności osób, których one dotyczą.
- 2nd Administrator odmawia udostępnienia danych, jeżeli spowodowałoby to naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.
- 3rd Powierzenie danych może nastąpić wyłącznie w drodze pisemnej umowy, w której podmiot przetwarzający dane zobowiązuje się do przestrzegania obowiązujących przepisów RODO. Umowa powinna zawierać informacje o podstawie prawnej powierzenia danych, celu i sposobie ich przetwarzania.
- 4th Administrator powinien korzystać z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi rozporządzenia i chroniło prawa osób, których dane dotyczą.
- 5th Administrator przed podpisaniem umowy głównej dotyczącej współpracy, np. w postępowaniu o udzielenie zamówienia publicznego, powinien wymagać od podmiotu przetwarzającego złożenia na etapie składania ofert, wypełnionej „ankiety dla podmiotu przetwarzającego” w celu dokonania oceny czy wykonawca zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie danych osobowych spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.
- 6th Administrator powinien stosować audyty jako najistotniejsze środki bezpieczeństwa. Konieczne jest zapewnienie regularnego monitoringu stosowanych zabezpieczeń oraz prowadzenia stałego nadzoru nad podmiotem przetwarzającym poprzez np. audyty i inspekcje.
- 7th Administrator jest odpowiedzialny za cykliczne, co najmniej raz w roku, przeprowadzenie audytu w podmiocie przetwarzającym.
- 8th Audyt w podmiocie przetwarzającym prowadzony jest według ankiety audytowej przygotowanej przez Inspektora Ochrony Danych – załącznik nr 15.

XXXVI. Współadministrowanie danymi osobowymi

- 1st Współadministrowanie danymi osobowymi następuje, gdy Administrator wraz z innym podmiotem wspólnie ustala cele i sposoby przetwarzania danych osobowych.
- 2nd W drodze pisemnej umowy zwanej „porozumienie o współadministrowaniu danymi osobowymi” Administratorzy określają:
 - 1) zakres swojej odpowiedzialności wynikającej z RODO, w szczególności w zakresie realizacji obowiązku informacyjnego, o którym mowa w rozdziale „Obowiązek informacyjny i wyrażenie zgody” oraz realizacji praw osób, których dane dotyczą;
 - 2) punkt kontaktowy dla osób, których dane dotyczą.
- 3rd Każdy przypadek współadministrowania danymi osobowymi powinien zostać skonsultowany i zatwierdzony przez Inspektora Ochrony Danych.

XXXVII. Postępowanie, gdy Administrator występuje jako podmiot przetwarzający

- 1st W niniejszym rozdziale Administrator rozumiany jest jako podmiot zewnętrzny powierzający dane osobowe.
- 2nd Podmiot przetwarzający jest zobowiązana stosować się do zapisów umowy powierzenia przetwarzania danych osobowych oraz RODO.
- 3rd Podmiot występujący w roli Administratora na każde żądanie otrzymuje od podmiotu przetwarzającego rejestr kategorii czynności przetwarzania obejmujący tylko powierzone dane osobowe.
- 4th Wszystkie osoby dopuszczone do przetwarzania danych osobowych otrzymują upoważnienie do przetwarzania danych osobowych zgodne z załącznikiem nr 1 lub ze wzorem zgodnym z umową. Wszystkie osoby upoważnione zobowiązane są do podpisania oświadczenia o zachowaniu poufności. Podmiot występujący w roli Administratora na każde żądanie otrzymuje od podmiotu przetwarzającego wykaz osób upoważnionych do przetwarzania powierzonych danych osobowych.
- 5th Notyfikacja incydentów bezpieczeństwa danych osobowych oraz informowania podmiot występujący w roli Administratora o zdarzeniach następuje zgodnie z umową powierzenia przetwarzania danych osobowych oraz rozdziałem „Postępowanie na wypadek wystąpienia naruszenia ochrony danych”.



6th W przypadku otrzymania wniosku od osoby, której dane dotyczą, należy niezwłocznie zawiadomić o tym fakcie podmiot występujący w roli Administratora. Sposób realizacji wniosku należy ustalić z podmiotem występującym w roli Administratora.

7th Zasady zwrotu i usunięcia danych osobowych reguluje umowa powierzenia przetwarzania danych osobowych. W przypadku braku właściwych zapisów w umowie zastosowanie mają procedury określone w niniejszej Polityce ochrony danych osobowych.

XXXVIII. Transfer danych poza Europejski Obszar Gospodarczy

1. Dane osobowe mogą być przekazywane poza Europejski Obszar Gospodarczy zgodnie z niniejszą Polityką Ochrony Danych Osobowych.
2. Niniejsze zasady dotyczą wszystkich operacji transferu danych osobowych poza EOG realizowanych przez Administratora, niezależnie od postaci danych osobowych (elektroniczna, papierowa) i celu przetwarzania.
3. Każdy przypadek transferu danych osobowych powinien zostać skonsultowany i zatwierdzony przez Inspektora Ochrony Danych.
4. Zanim dojdzie do transferu danych osobowych należy ustalić, czy:
 - 1) Komisja Europejska (dalej KE) wydała decyzję stwierdzającą odpowiedni stopień ochrony danych w danym państwie (art. 45 RODO);
 - 2) W przypadku braku takiej decyzji – czy możliwe jest zastosowanie odpowiednich zabezpieczeń (art. 46 RODO), takich jak:
 - a) Standardowe klauzule umowne,
 - b) Wiążące reguły korporacyjne,
 - c) Kodeksy postępowania lub mechanizmy certyfikacji.

Jeżeli nie można zapewnić żadnej z powyższych podstaw, transfer może odbyć się jedynie w oparciu o wyjątki opisane w art. 49 RODO, np. na podstawie wyraźnej zgody osoby, której dane dotyczą, ze względu na ważne względy interesu publicznego, w celu ustalenia, dochodzenia lub obrony roszczeń.

5. Dla każdego transferu z wykorzystaniem standardowych klauzul i innych środków zabezpieczających na podstawie art. 46 RODO, należy przeprowadzić Transfer Impact Assessment (TIA). TIA przeprowadzane jest za pomocą wzoru raportu dostarczonego przez IOD.
6. Każdy transfer należy odpowiednio udokumentować za pomocą:
 - 1) umów zawierających standardowe klauzule umowne lub innych środków zabezpieczających np. wiążących reguł korporacyjnych, zatwierdzonego kodeksu postępowania, zatwierdzonego mechanizmu certyfikacji,
 - 2) raportu z oceny skutków transferu (TIA),
 - 3) zgody osób, których dane dotyczą, jeśli jest ona podstawą transferu,

Transfer danych osobowych należy odnotować w rejestrze czynności przetwarzania danych osobowych.

7. Osoby, których dane dotyczą muszą zostać poinformowane o fakcie przekazania ich danych osobowych poza EOG.
8. Transfery danych osobowych powinny być regularnie weryfikowane pod kątem:
 - 1) aktualności decyzji Komisji Europejskiej,
 - 2) obowiązujących przepisów prawa Państwa Trzeciego,
 - 3) efektywności zastosowanych zabezpieczeń.

H. Załączniki

- Załącznik nr 1 – Wzór upoważnienia do przetwarzania danych osobowych.
- Załącznik nr 2 – Rejestr osób upoważnionych do przetwarzania danych osobowych.
- Załącznik nr 3 – Oświadczenie o zapoznaniu się z zasadami zachowania bezpieczeństwa danych osobowych.
- Załącznik nr 4 – Wzór rejestru naruszeń ochrony danych osobowych.
- Załącznik nr 5 – Raport z naruszenia bezpieczeństwa danych osobowych.
- Załącznik nr 6 – Rejestr zawartych umów powierzenia przetwarzania danych osobowych.
- Załącznik nr 7 – Katalog przykładowych naruszeń.
- Załącznik nr 8 – Wniosek o realizację praw RODO.
- Załącznik nr 9 – Procedura ochrony danych osobowych w trakcie pracy zdalnej.
- Załącznik nr 10 – Zasady prowadzenia Biuletynu Informacji Publicznej (BIP), zasady publikacji, aktualizacji oraz okresowych przeglądów danych zamieszczanych w Biuletynie Informacji Publicznej.
- Załącznik nr 11 – Wykaz przykładowych działań dotyczących testowania środków technicznych i organizacyjnych.
- Załącznik nr 12 – Analiza zagrożeń i ryzyka – wzór i metodologia.
- Załącznik nr 13 – Procedura anonimizacji danych osobowych.
- Załącznik nr 14 – Rejestr sprzętu służącego do przetwarzania danych osobowych.
- Załącznik nr 15 – Audyt podmiotów przetwarzających.

DYREKTOR
Miejskiego Centrum Kultury, Sportu i Rekreacji
im. Ryszarda Kaczorowskiego w Raciążu

Robert Szymborski



