Załącznik
do uchwały nr 01/05/2024
Zarządu Klubu Sportowego Delta Warszawa
z 06 maja 2024 r.
w sprawie przyjęcia polityki ochrony danych osobowych

# POLITYKA
# OCHRONY DANYCH OSOBOWYCH
# KLUBU SPORTOWEGO DELTA WARSZAWA

## Spis treści

## PODSTAWY PRAWNE

§1

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

## PODSTAWOWE POJĘCIA

§2

1. Administrator (ADO) - w tym dokumencie jest rozumiany jako Klub Sportowy Delta Warszawa.
2. 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).
3. Polityka - w tym dokumencie jest rozumiana jako „Polityka Ochrony Danych Osobowych" obowiązująca u Administratora.
4. Inspektor Ochrony Danych (IOD) - osoba wyznaczona przez Administratora do nadzorowania przestrzegania zasad ochrony danych osobowych oraz przygotowania dokumentów wymaganych przez RODO. IOD powołany jest uchwałą Zarządu Administratora.
5. 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.

## Cele i zasady funkcjonowania Polityki ochrony danych osobowych

§3

1. 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.

§4

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.

§5

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.

**Zasady przetwarzania danych osobowych**

§6

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 danej 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 pracownicy 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) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe (obszar przetwarzania danych osobowych),
g) rejestr czynności przetwarzania danych dokumentujący podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania,
h) rejestr kategorii czynności przetwarzania danych osobowych,
i) upoważnienia do przetwarzania danych osobowych; wzór upoważnienia stanowi załącznik numer 1 do niniejszej Polityki,
j) ewidencję osób upoważnionych do przetwarzania danych osobowych; wzór ewidencji stanowi załącznik numer 2 do niniejszej Polityki,
k) oświadczenia o zachowaniu poufności; wzór oświadczenia stanowi załącznik numer 3 do niniejszej Polityki,
l) umowy z podmiotami, którym powierzono przetwarzanie danych, w tym rejestr zawartych umów; wzór rejestru stanowi załącznik numer 6 do niniejszej Polityki,
m) inne rozwiązania organizacyjne i techniczne, określone w załącznikach do niniejszej Polityki oraz innych wewnętrznych regulacji.

8) Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach:
Administrator nie podejmuje decyzji w indywidualnych przypadkach, które opierają się wyłącznie na zautomatyzowanym przetwarzaniu.

**Zasady bezpiecznego użytkowania sprzętu IT, dysków, programów**

§7

1. 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.
2. Użytkownik ma obowiązek natychmiast zgłosić zagubienie, utratę lub zniszczenie powierzonego mu sprzętu IT.
3. Samowolne otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) do lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.
4. Użytkownik jest zobowiązany do zabezpieczenia pamięci zewnętrznych hasłem zgodnie z zasadami opisanymi paragrafie „Polityka haseł”.
5. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym wglądu do danych wyświetlanych na monitorach komputerowych.
6. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (na przykład poprzez użycie skrótu WINDOWS + L) lub wylogować się z systemu bądź z programu.
7. 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.
8. Użytkownik może odstąpić od zasady określonej w ust. 7, tylko na polecenie Administratora np. w przypadku pracy zdalnej.
9. 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).
10. Jeśli użytkownik jest uprawniony do niszczenia nośników, powinien trwale zniszczyć sam nośnik lub trwale usunąć z niego dane (np. zniszczenie płyt DVD w niszczarce, zniszczenie twardego dysku, pendrive młotkiem).
11. Użytkownicy komputerów przenośnych, na których znajdują się dane osobowe lub z dostępem do danych osobowych przez Internet zobowiązani są do stosowania zasad bezpieczeństwa.
12. Niedozwolone jest zabezpieczanie sprzętu IT przez użytkowników blokadami posługującymi się danymi biometrycznymi (np. odcisk palca, rozpoznawanie twarzy). Możliwymi do zastosowania zabezpieczeniami są m.in. kod PIN oraz wzór blokady.
13. W 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.

14. Nie wolno włączać synchronizacji z chmurami, które nie są własnością Administratora (np. zakazana jest synchronizacja telefonu służbowego z prywatnym kontem Google).
15. W 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.
16. Administrator lub osoba przez niego wyznaczona np. informatyk, zobowiązany jest do monitorowania i analizy logów systemowych oraz aplikacyjnych pod kątem wystąpienia niepożądanych zdarzeń.
17. Administrator lub osoba przez niego wyznaczona np. informatyk, zobowiązany jest do bieżącej aktualizacji routerów.

**Zarządzanie uprawnieniami**

§8

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

**Polityka haseł**

§9

1. Hasła powinny składać się z min. 8 znaków zawierając małe i duże litery, cyfry i symbole lub powinny się składać z co najmniej 16 znaków zawierając 4-5 losowych wyrazów.
2. 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.
3. Hasła nie powinny być ujawnianie innym osobom.
4. Nie wolno zapisywać haseł na kartkach i w notesach, naklejać na monitorze komputera, trzymać pod klawiaturą lub w szufladzie.
5. W przypadku ujawnienia hasła - należy natychmiast je zmienić, a fakt ujawnienia zgłosić Administratorowi i Inspektorowi Ochrony Danych.
6. 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.
7. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła.
8. 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).
9. Jeśli zastosowana zostanie metoda uwierzytelniania dwustopniowego przy logowaniu to zmiana hasła, określona w ust. 6, nie jest wymagana.

**Zabezpieczenie dokumentacji papierowej z danymi osobowymi**

§10

1. Upoważnieni pracownicy 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.
2. Upoważnieni pracownicy zobowiązani są do bezpiecznego niszczenia dokumentów i wydruków na przykład w niszczarkach odpowiedniej jakości (niszczarka od poziomu P-4 tak zwana „strzępkowa”).
3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. na korytarzach, kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych.
4. Zabrania się wyrzucania niezniszczonych dokumentów do śmietnika lub porzucania ich na zewnątrz, np.: na

terenach publicznych, miejskich lub w lesie.

5. 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.

**Zasady wynoszenia nośników z danymi poza siedzibę Administratora**

§11

1. Użytkownicy nie mogą wynosić poza siedzibę Administratora wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Administratora.
2. Dane osobowe wynoszone poza siedzibę Administratora muszą być zaszyfrowane (szyfrowane dyski, pliki). Za prawidłowe zabezpieczenie nośnika odpowiada Administrator.
3. Użytkownik przewożący dokumenty jest zobowiązanych do ich zabezpieczenia przed zgubienie, kradzieżą lub innym nieuprawnionym dostępem.
4. Należy korzystać ze sprawdzonych firm kurierskich.

**Zasady korzystania z Internetu**

§12

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia 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.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez nieautoryzowane oprogramowanie instalowane z Internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera).
5. Zabrania się logowania na prywatne konta między innymi pocztę e-mail, portale społecznościowe. Ten zakaz nie obowiązuje jeśli Administrator wyda pisemną zgodę na logowanie do tego typu serwisów.
6. 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.
7. 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 tyczy się to żądania podania takich informacji przez rzekomy bank.
8. Należy zweryfikować poprawność adresu strony internetowej, na której podawane będą dane uwierzytelniające lub dane osobowe.
9. Zabrania się korzystania z publicznych sieci WiFi, a w przypadku niepublicznych sieci dopuszcza się korzystanie tylko w sytuacji, gdy są odpowiednio zabezpieczone.
10. Zabrania się korzystania z menadżera haseł dostępnego z poziomu przeglądarki internetowej, w tym korzystania z opcji autouzupełniania.

**Zasady korzystania z poczty elektronicznej**

§13

1. Przesyłanie danych osobowych z użyciem e-maila poza strukturę Administratora może odbywać się tylko przez osoby do tego upoważnione.
2. W przypadku przesyłania danych osobowych poza strukturę Administratora należy wykorzystywać mechanizmy kryptograficzne (szyfrowanie wysyłanych dokumentów lub plików zzipowanych, podpis elektroniczny).
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 6 znaków: litery i cyfry, a hasło należy przesłać odrębnym środkiem komunikacji lub inną metodą, np. telefonicznie lub SMS-em.
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
5. 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.

6. 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.
7. Należy zgłaszać Administratorowi przypadki podejrzanych e-maili.
8. Użytkownicy nie powinni rozsyłać „niezawodowych” e-maili w formie „łańcuszków szczęścia", np. życzenia świąteczne adresowane do 230 osób.
9. 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.
10. Użytkownicy powinni okresowo kasować niepotrzebne e-maile, zgodnie z zasadami dotyczącymi okresu przechowywania danych osobowych obowiązującymi u Administratora.
11. Każda osoba, która przetwarza dane osobowe w imieniu Administratora, wykorzystuje w tym celu jedynie e-mail służbowy.
12. E-mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.
13. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.
14. Przy korzystaniu z e-maila, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
15. Użytkownicy nie mają prawa korzystać z e-maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.
16. Użytkownik bez zgody Administratora nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Administratora, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.
17. 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 pracownika, 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.
18. Zakazuje się łączenia poczty służbowej z pocztą prywatną np. poprzez przekierowanie wiadomości e-mail.
19. Użytkownik bez zgody Administratora nie może korzystać z poczty prywatnej na sprzęcie służbowym.
20. W przypadku konieczności wykonywania pracy na odległość (np. praca zdalna, delegacja) pracownicy są obowiązani stosować się do zasad określonych w polityce ochrony danych osobowych.

**Ochrona antywirusowa**

§14

1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym, jeśli system antywirusowy taką funkcje posiada.
2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.
3. 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.
4. Baza wirusów w programie antywirusowym musi być na bieżąco aktualizowana.

**Procedura wykonywania przeglądów, konserwacji, napraw sprzętu IT, systemów służących do przetwarzania danych osobowych**

§15

1. Przeglądy, konserwacja, naprawy baz danych, oprogramowania, sprzętu IT przeprowadzana jest przez Administratora lub osobę upoważnioną. Dopuszczalne jest zaangażowanie firmy zewnętrznej.
2. 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 zdemontować dyski i zabezpieczyć je u Administratora (na przykład na czas naprawy);
3) należy zgrać dane na inny nośnik i usunąć je z przekazywanego sprzętu.

3. Jeśli firma zewnętrzna dokonująca przeglądu, konserwacji, naprawy oprogramowania, sprzętu IT otrzymuje dostęp do danych osobowych należy zawrzeć umowę powierzenia.
4. 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.
5. W przypadku złomowania sprzętu komputerowego, nośniki informacji (dyski twarde) są fizycznie niszczone przez Administratora lub osobę upoważnioną.

**Bezpieczeństwo wymiennych nośników informacji**

§16

1. Przez wymienne nośniki informacji rozumie się: taśmy, pamięci typu flash, pendrive USB, wyjmowane dyski twarde, przenośne dyski twarde USB, płyty CD i DVD oraz wydruki.
2. Użytkownik systemów informatycznych u Administratora używając wymiennych nośników informacji bezwzględnie stosuje następujące zasady:
   1) zabrania się wynoszenia danych osobowych z systemu informatycznego Administratora, zapisywanych na wymiennych nośnikach danych poza siedzibę Administratora;
   2) wymienne nośniki danych, które zawierają dane osobowe, są przechowywane w pokojach biurowych stanowiących obszar przetwarzania danych osobowych;
   3) 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;
   4) 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;
   5) 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;
   6) za nośnik danych i bezpieczeństwo zapisanych na nim danych odpowiada Użytkownik;
   7) wycofane nośniki informacji, nie mogą być wynoszone poza obszary przetwarzania danych u Administratora bez wcześniejszego skutecznego usunięcia danych.
3. Uszkodzone wymienne nośniki informacji, są niszczone przez upoważnione osoby przez Administratora w sposób uniemożliwiający odczytanie zapisanych na nich danych.
4. Wycofanie z eksploatacji wymiennych nośników informacji, przekazanie do naprawy lub ponownego użycia, jest poprzedzone archiwizacją, a następnie skutecznym usunięciem zapisanych danych.
5. W przypadku zgubienia nośnika z danymi, fakt ten musi zostać zgłoszony do bezpośredniego przełożonego oraz do IOD.
6. Zabrania się używania prywatnych zewnętrznych nośników komputerowych lub nośników niewiadomego pochodzenia w infrastrukturze systemów informatycznych Administratora.
7. Wszystkie niezautoryzowane wymienne nośniki informacji mają zablokowany dostęp do infrastruktury Administratora.
8. W przypadku konieczności zapisu/odczytu informacji na wymiennym nośniku informacji dostarczonych przez kontrahenta Administratora, pracownik musi skontaktować się z osobą wyznaczoną np. informatykiem, w celu umożliwienia dostępu do danych znajdujących się na nośniku.
9. 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 (pamięć USB, dysk twardy, itp.) zostanie uszkodzony i nie można go odczytać ani usunąć

z niego danych, to należy go zniszczyć mechanicznie.

10. W przypadku przekazania sprzętu komputerowego do naprawy lub konserwacji stronie trzeciej, w którym demontaż nośnika informacji powoduje utratę gwarancji dopuszcza się przekazanie sprzętu z zaszyfrowanym dyskiem.

**Procedura tworzenia kopii zapasowych**

§17

1. Kopie całościowe sporządzane są raz w miesiącu.
2. Kopie sporządzane są na dyskach zewnętrznych lub płycie DVD/CD.
3. Każda nośnik jest opisany datą jej sporządzenia.
4. Kopie zapasowe przechowywane są tak długo jak wymagają tego przepisy prawa.
5. Dostęp do kopii mają osoby upoważnione przez Administratora.
6. Kopie przechowywane są miejscu zabezpieczonym na terenie siedziby Administratora.
7. Wykonane kopie zapasowe podlegają testowaniu, mierzeniu i ocenianiu nie rzadziej niż raz na 3 miesiące. Protokół potwierdzający wykonanie czynności sporządza i przechowuje informatyk.
8. Kopie zapasowe należy przechowywać na co najmniej dwóch różnych nośnikach, w tym jedną z nich w wersji offline (np. na płycie CD).

**Procedura zarządzania zmianą w systemie, który nie jest własnością Administratora (Administrator korzysta ze wsparcia podmiotu – podmiot przetwarzający)**

§18

1. Obowiązki Administratora w stosunku do podmiotu przetwarzającego opisane zostały w paragrafie „Udostępnianie i powierzanie danych osobowych”. .
2. 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.
3. Zmiana w systemie powinna zostać w sposób formalny (np. pisemne powiadomienie o konieczności wprowadzenia zmiany) zainicjowana przez Administratora lub podmiot przetwarzający - ustalenie celu zmiany.
4. Komórka organizacyjna podmiotu przetwarzającego odpowiedzialna za wdrożenie zmian przygotowuje oraz w jasny i czytelny sposób przedstawia plan zmian w systemie, w szczególności obszarów, które mogą mieć wpływ na bezpieczeństwo danych osobowych do rekomendacji inspektora ochrony danych, radcy prawego oraz osoby wyznaczonej np. informatyka.
5. Po uzyskaniu rekomendacji inspektora ochrony danych osobowych, radcy prawnego oraz osoby wyznaczonej np. informatyka, plan zmian w systemie zatwierdza Administrator.
6. Za bezpieczne wdrożenie zmian odpowiada wskazana przez Administratora komórka organizacyjna.
7. Administrator i podmiot przetwarzający odpowiadają za testowanie zmian, w szczególności za sprawdzenie bezpieczeństwa systemu i czy wszystkie problemy systemowe zostały rozwiązane.
8. Testowanie systemów może odbyć się wyłącznie w środowisku testowym, tj. poza pracą bieżącą systemów.
9. Zabrania się stosowania danych rzeczywistych w charakterze danych testowych.
10. Administrator i podmiot przetwarzający mają obowiązek:
    1) ewidencjonowania zmian wprowadzanych w systemach, wspomagania zarządzania projektami i ich kontroli;
    2) stosować ochronę danych osobowych na etapie projektowania zmian w systemie;
    3) przeprowadzania regularnych przeglądów bezpieczeństwa danych osobowych w systemie, nie rzadziej niż raz w roku;
    4) przechowywania dokumentacji dowodowej z przeprowadzanych audytów zabezpieczeń oraz środków technicznych i organizacyjnych.
11. 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.

**Regulamin użytkowania komputerów przenośnych**

§19

1. Każdy użytkownik komputera przenośnego powinien zapoznać się z niniejszym Regulaminem użytkowania komputerów przenośnych.
2. W przypadku przechowywania na komputerze przenośnym danych osobowych lub stanowiących tajemnicę Administratora, użytkownik zobowiązany jest do ich przechowywania na dysku szyfrowanym, zabezpieczonym hasłem zgodnym z „Polityką haseł".
3. Na komputerach przenośnych przeznaczonych do zewnętrznych prezentacji multimedialnych nie powinny, o ile jest to możliwe, znajdować się dane osobowe lub stanowiące tajemnicę Administratora.
4. W przypadku kradzieży lub zgubienia sprzętu IT, użytkownik powinien natychmiast powiadomić Administratora lub IOD, zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane.
5. Użytkownik zobowiązany jest do zabezpieczenia komputera przenośnego w czasie transportu, a w szczególności:
   1) 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;
   2) zabrania się pozostawiania komputera przenośnego w samochodzie podczas postoju w miejscu publicznym bez nadzoru. Złodzieje dysponują aparaturą umożliwiającą wykrywanie nawet ukrytych komputerów przenośnych;
   3) 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.
6. W 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.
7. W przypadku pozostawiania komputerów przenośnych w biurze zaleca się umieszczanie ich po zakończeniu pracy w zamykanych szafkach.
8. Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych.

**Procedura postępowania na wypadek wystąpienia naruszenia ochrony danych**

§20

1. 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.
2. Katalog przykładowych zagrożeń i naruszeń, jakie mogą wystąpić w związku z przetwarzaniem danych znajduje się w załączniku nr 7 do niniejszej Polityki.
3. 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 24 godzin od zaistnienia sytuacji. Osoba stwierdzająca naruszenie musi uzupełnić raport, który stanowi załącznik nr 5 do niniejszej Polityki.
4. Osoba, która stwierdzi fakt naruszenia ma obowiązek podjąć działania niezbędne do powstrzymania skutków naruszenia oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn i skutków naruszenia.
5. Administrator podejmuje działania w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w celu zminimalizowania jego ewentualnych negatywnych skutków.
6. 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.

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

**Analiza wystąpienia ryzyka naruszenia praw i wolności osób fizycznych**

§21

1. Administrator „stwierdza" naruszenie, kiedy ma on wystarczający stopień pewności co do tego, że miało miejsce zdarzenie zagrażające bezpieczeństwu, które doprowadziło do naruszenia ochrony danych.
2. 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.
3. Administrator dokonuje analizy każdorazowo w odniesieniu do konkretnego naruszenia.
4. 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.
5. Stopień dotkliwości w przypadku zmaterializowania się zagrożenia należy oceniać z perspektywy osób, których dane są przetwarzane.
6. 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.
7. Nie jest konieczne, aby ryzyko się zmaterializowało (by faktycznie doszło do naruszenia). Należy ocenić prawdopodobieństwo zaistnienia szkody w przypadku danego zdarzenia.
8. W przypadku jakichkolwiek wątpliwości Administrator powinien zgłosić naruszenie, nawet jeśli taka ostrożność mogłaby się okazać nadmierna.
9. 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.
10. 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.
11. 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.

12. 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 (ŁI) – 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.
13. 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) Ocenić występowanie czynników bądź zakresów danych, które zwiększają lub zmniejszają wynik podstawowy.
14. Łatwość identyfikacji ocenia jak łatwo będzie dla strony, która ma dostęp do zestawu danych, jednoznacznie dopasować je do określonej osoby. Wyróżniamy cztery poziomy ŁI: znikome (0,25 pkt.), ograniczone (0,5 pkt.), znaczące (0,75 pkt.) i maksymalne (1,0 pkt.).
15. Przy określaniu okoliczności naruszenia należy brać pod uwagę utratę poufności, integralności i dostępności danych oraz złośliwe zamiary, które uzupełniają KPD i ŁI 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 bezprawny 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 włamania, 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.
16. Końcowy wynik oceny dotkliwości naruszenia oblicza się wzorem: (DN): DN=KPDxŁI+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 numer 4 do niniejszej Polityki.

**Obowiązek zachowania poufności i ochrony danych osobowych**

§22

1. 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.

2. Osoba dopuszczona do przetwarzania musi zostać przeszkolona z zasad ochrony danych osobowych, przed wydaniem upoważnienia do przetwarzania danych osobowych.
3. Osoby zapoznane z treścią niniejszej Polityki lub przeszkolone zobowiązane są podpisać oświadczenie o poufności, które stanowi załącznik numer 3.
4. 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.
5. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.
6. 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 nadzorczemu, którym jest Prezes Urzędu Ochrony Danych Osobowych.
7. 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.
8. 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.
9. 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.

**Postępowanie dyscyplinarne**

§23

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 i ustawie.

**Polityka kluczy**

§24

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

**Udostępnianie i powierzanie danych osobowych**

§25

1. 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.

2. Administrator odmawia udostępnienia danych, jeżeli spowodowałoby to naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.
3. 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.
4. 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.
5. 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.
6. 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.
7. Administrator jest odpowiedzialny za cykliczne, co najmniej raz w roku, przeprowadzenie audytu w podmiocie przetwarzającym.
8. Audyt w podmiocie przetwarzającym prowadzony jest według ankiety audytowej przygotowanej przez Inspektora Ochrony Danych.

**Współadministrowanie danymi osobowymi**

§26

1. Współadministrowanie danymi osobowymi następuje, gdy Administrator wraz z innym podmiotem wspólnie ustala cele i sposoby przetwarzania danych osobowych.
2. 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 paragrafie „Obowiązek informacyjny i wyrażenie zgody" oraz realizacji praw osób, których dane dotyczą;
   2) punkt kontaktowy dla osób, których dane dotyczą.
3. Każdy przypadek współadministrowania danymi osobowymi powinien zostać skonsultowany i zatwierdzony przez Inspektora Ochrony Danych.

**Obowiązek informacyjny i wyrażenie zgody**

§27

1. Każdy pracownik, który zbiera dane osobowe w imieniu Administratora, jest zobowiązany do przekazania zainteresowanemu obowiązku informacyjnego.
2. Dedykowany obowiązek informacyjny powinien być zamieszczony w każdym miejscu, gdzie są zbierane dane osobowe (np. na stronie internetowej, w postępowaniu przetargowym, w formularzach zgłoszeniowych).
3. 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.
4. 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.
5. 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 zmieniłby się przedmiot i charakter przedstawienia.

**Projektowanie prywatności**

§28

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 zaprojektowana bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub inwestycji.

**Procedura postępowania, gdy Administrator występuje jako podmiot przetwarzający**

§29

1. W niniejszym paragrafie Administrator rozumiany jest jako podmiot zewnętrzny powierzający dane osobowe.
2. Podmiot przetwarzający jest zobowiązana stosować się do zapisów umowy powierzenia przetwarzania danych osobowych oraz RODO.
3. Podmiot występujący w roli Administratora na każde żądanie otrzymuje od podmiotu przetwarzającego rejestr kategorii czynności przetwarzania obejmujący tylko powierzone dane osobowe.
4. 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.
5. Notyfikacja incydentów bezpieczeństwa danych osobowych oraz informowania podmiot występujący w roli Administratora o zdarzeniach następuje zgodnie z umową powierzenia przetwarzania danych osobowych oraz paragrafem „Procedura postępowania na wypadek wystąpienia naruszenia ochrony danych".
6. 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.
7. 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.

**Prawa osób, których dane dotyczą**

§30

1. Osoba, której dotyczą przetwarzane przez Administratora dane osobowe, ma prawa wynikające z Rozporządzenia.
2. 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.
3. Prawo do sprostowania danych – uprawnienie do niezwłocznego sprostowania przez Administratora danych osobowych osoby, które nie są prawidłowe lub uzupełnienia niekompletnych danych osobowych.
4. 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.

   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.
5. 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.

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 uchyleniem ograniczenia przetwarzania zgodnie z ust. 2, Administrator informuje o tym osobę, której dane dotyczą, która żądała ograniczenia.

6. 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.
   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 przekaże kopię tych danych na wskazany przez nią adres.
7. 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.
8. Prawo do niepodlegania profilowaniu – uprawnienie do niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowanych przetwarzaniu, w tym profilowani i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.
9. Osoba, o której mowa w ust. 1 powyżej może złożyć do Administratora wniosek dotyczący skorzystania z praw, które jej przysługują. Wzór wniosku stanowi załącznik numer 8 do niniejszej Polityki.
10. Jeśli osoba, o której mowa w ust. 1 złoży wniosek w innej formie niż wskazany w ust. 9 powyżej Administrator jest zobowiązany do jego realizacji.

**Procedura usuwania i prostowania danych**

§31

1. Pracownicy Administratora usuwając dane osobowe muszą skorzystać:
   1) w przypadku danych przetwarzanych w formie papierowej (np. dokumenty, ale też wszelkie notatki, kalendarze itp.) wykorzystując niszczarkę;
   2) w przypadku danych zapisanych na nośnikach danych, należy postąpić zgodnie z paragrafem „bezpieczeństwo wymiennych nośników informacji".
2. Jeżeli do Administratora wpłynie wniosek o usunięcie danych, to po sprawdzeniu czy dane osobowe nie są niezbędne:
   1) do korzystania z prawa do wolności wypowiedzi i informacji;
   2) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega Administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi;
   3) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego;

4) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, o ile prawdopodobne jest, że prawo uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania;
5) do ustalenia, dochodzenia lub obrony roszczeń;

usuwa je zgodnie z zapisami ust. 1.

3. Jeżeli zachodzi jedna z przesłanek, opisanych w ust. 2, Administrator odmawia usunięcia danych.
4. Przez wniosek o usunięcie danych rozumie się również otrzymaną wiadomość e-mail, która wyłącznie w tytule zawiera żądanie usunięcia danych bez dodatkowej treści w dalszej części wiadomości.
5. Osoba, której dane dotyczą, ma prawo żądania od Administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.
6. W przypadku opisanym w ust. 5 Administrator wprowadza niezbędne zmiany w danych, w posiadaniu, których jest.
7. Administrator zwraca uwagę na różnice w okresach retencji danych osobowych w stosunku do danych przetwarzanych za pomocą różnych środków (elektronicznych, papierowych) i usuwa je po upływie określonego okresu, zgodnie z przepisami prawa lub umowami powierzenia przetwarzania danych.
8. Administrator oraz osoba wyznaczona (np. osoba zajmująca się archiwizacją) ponoszą odpowiedzialność za przestrzeganie okresów retencji (archiwizacji) dokumentacji zawierającej dane osobowe i usuwanie jej w terminie zgodnym z obowiązującymi przepisami prawa lub w przypadku braku takich uregulowań, z ustalonymi okresami niezbędnymi do realizacji celów, dla których dane są przetwarzane.
9. Powyższa procedura odnosi się także do usuwania wizerunku na nagraniach, zdjęciach, publikacjach.

**Monitoring wizyjny**

§32

1. Administrator musi na swoim terenie poinformować o monitoringu, poprzez zmieszczenie wyraźniej informacji na drzwiach, korytarzach, płotach itp. 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.
2. W przypadku stosowania wideodomofonu należy umieścić informację, że następuje monitoring w czasie rzeczywistym np. w zakresie wizji i dźwięku.
3. Należy zastosować obowiązek informacyjny, o którym mowa w paragrafie „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.
4. 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.
5. Okres przechowywania danych po dokonaniu nagrania nie może być dłuższy niż 30 dni.
6. Do ekranu, na którym odtwarzany jest monitoring mają dostęp tylko osoby upoważnione przez Administratora.
7. Rejestrator monitoringu jest obowiązkowo przechowywany w miejscu zamkniętym dla osób trzecich, a dostęp do niego mają tylko osoby upoważnione przez Administratora.
8. 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.
9. Stosowanie monitoringu dozwolone jest w celu: zapewnienia bezpieczeństwa, ochrony mienia, kontroli produkcji,

zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę.

10. Monitoringu nie można stosować w celu: nadzoru nad jakością wykonywania pracy.
11. Niedozwolone jest instalowanie atrap kamer monitoringu.
12. 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.

**Identyfikacja obszarów wymagających szczególnych zabezpieczeń**

§33

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.

**Załączniki**

Załącznik nr 1 - Wzór upoważnienia do przetwarzania danych osobowych.
Załącznik nr 2 - Rejestr osób upoważnionych do przetwarzania danych osobowych.
Załącznik nr 3 - Oświadczenie pracownika o zapoznaniu się z zasadami zachowania bezpieczeństwa danych osobowych.
Załącznik nr 4 - Rejestr 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 1**

Warszawa, dn. ……

**UPOWAŻNIENIE NR ….**
**DO PRZETWARZANIA DANYCH OSOBOWYCH**

Działając w imieniu Klubu Sportowego Delta Warszawa na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE oraz innych przepisów upoważniam:

……
*(imię, nazwisko, stanowisko)*

do przetwarzania danych osobowych w następującym zakresie:

zawodnicy klubu/pełen zakres
*(tu należy wskazać odpowiedni zakres przetwarzanych danych osobowych, określonych w analizie ryzyka w dziale „aktywa podstawowe")*

Niniejsze upoważnienie jest wydane na czas oznaczony do dnia zakończenia pracy osoby upoważnionej w Klubie Sportowym Delta Warszawa.

……
*(podpis osoby działającej w imieniu Administratora Danych Osobowych)*

**Załącznik nr 2**

**REJESTR OSÓB UPOWAŻNIONYCH**

**DO PRZETWARZANIA DANYCH OSOBOWYCH**

| L.p. | Imię i nazwisko | Zakres upoważnienia do przetwarzania danych osobowych | Data nadania uprawnień | Data odebrania uprawnień | Uwagi |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

**Załącznik nr 3**

……, dn. ……

……
*(imię i nazwisko )*

**OŚWIADCZENIE**
**o zachowaniu poufności i zapoznaniu się z przepisami**

Ja niżej podpisana/y oświadczam, iż zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań i obowiązków służbowych wynikających ze zobowiązań wobec Klubu Sportowego Delta Warszawa, zarówno w czasie trwania relacji (m.in. umowy, porozumienia), jak i po jej ustaniu.

Oświadczam, że zostałam/em poinformowany/a o obowiązujących zasadach dotyczących przetwarzania danych osobowych, określonych w Polityce ochrony danych osobowych i zobowiązuję się ich przestrzegać.

Zostałam/em zapoznana/y z przepisami o ochronie danych osobowych. Poinformowano mnie również o grożącej, stosownie do przepisów odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, że złamanie zasad ochrony danych osobowych, obowiązujących w Klubie Sportowym Delta Warszawa może zostać uznane za ciężkie naruszenie podstawowych obowiązków i skutkować odpowiedzialnością.

……..……
*(data i podpis osoby upoważnionej)*

**Załącznik nr 5**

……, dnia …… r.

## RAPORT Z NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. Data i godzina: ..... r.
2. Osoba powiadamiająca o zaistniałym zdarzeniu: …… .....
   *(imię, nazwisko, stanowisko służbowe)*
3. Lokalizacja zdarzenia: ……
   *(np. nr pokoju, nazwa pomieszczenia, poczta elektroniczna)*
4. Kategorie osób, których dotyczy naruszenie i rodzaj danych osobowych:

| **Kategorie osób** | **Liczba osób** | **Rodzaj danych osobowych** |
|---|---|---|
| np. pracownicy | | Nazwiska i imiona, imiona rodziców, data urodzenia, numer rachunku bankowego, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, adres e-mail, nazwa użytkownika i/lub hasło, dane dotyczące zarobków i/lub posiadanego majątku, nazwisko rodowe matki, seria i numer dowodu osobistego, numer telefonu, wizerunek, dane o pochodzeniu rasowym lub etnicznym, dane o poglądach politycznych, dane o przekonaniach religijnych lub światopoglądowych, dane o przynależności do związków zawodowych, dane dotyczące seksualności lub orientacji seksualnej, dane dotyczące zdrowia, dane genetyczne, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące wyroków skazujących, dane dotyczące czynów zabronionych, inne (jakie?)* |
| | | |
| | | |

5. Dokładny opis naruszenia:
   .....
   .....
   .....
6. Przyczyny wystąpienia zdarzenia:
   .....
   .....
7. Podjęte działania:
   .....
   .....
8. Czy powiadomiono organy ścigania? TAK/NIE

.....
*(data i podpis zgłaszającego)*

*Niepotrzebne usunąć

**Załącznik nr 6**

**REJESTR ZAWARTYCH UMÓW POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH**

| L.p. | Podmiot, z którym została zawarta umowa | Data zawarcia umowy | Data rozwiązania umowy | Uwagi |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

**Załącznik nr 7**

## KATALOG PRZYKŁADOWYCH NARUSZEŃ

1. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych np. brak haseł, brak oprogramowania antywirusowego;
2. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników np. niestosowanie zasady czystego biurka, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek;
3. pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności;
4. awarie serwera, komputerów, twardych dysków, oprogramowania;
5. pomyłki informatyków, użytkowników;
6. włamanie do systemu informatycznego lub pomieszczeń;
7. kradzież danych/sprzętu;
8. świadome zniszczenie dokumentów/danych;
9. działanie wirusów i innego szkodliwego oprogramowania np. poprzez szyfrowanie plików znajdujących się na urządzeniu;
10. ślady na drzwiach, oknach i szafach wskazujące na próbę włamania;
11. niszczenie dokumentacji bez użycia niszczarki;
12. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie;
13. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe;
14. ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe;
15. wynoszenie danych osobowych w wersji papierowej i elektronicznej poza siedzibę Administratora bez upoważnienia Administratora;
16. zgubienie dokumentów przy ich przewożeniu;
17. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej;
18. telefoniczne próby wyłudzenia danych osobowych;
19. kradzież, zagubienie komputerów lub CD, twardych dysków, pendrive z danymi osobowymi;
20. przekazanie danych dostępowych w odpowiedzi na e-maile zachęcające do ujawnienia identyfikatora i/lub hasła;
21. kliknięcie w link/załącznik zawierający wirusa;
22. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;
23. hasła do systemów przyklejone są w pobliżu komputera;
24. utrata lub zagubienie danych np. chwilowe pozostawienie nośnika z danymi osobowymi w miejscu publicznym;
25. używanie poczty e-mail, „chmur" w serwisach, które nie są dostosowane do przepisów o ochronie danych osobowych;
26. przesyłanie danych osobowych (w szczególności danych wrażliwych) w niezaszyfrowanym e -mailu;
27. ujawnienie danych osobowych przez osobę, która została zwolniona z pracy lub została zobowiązana do zachowania poufności;
28. udzielenie odpowiedzi na pismo policji/urzędu/innej jednostki, w którym nie została przywołana podstawa prawna działań;
29. wykorzystywanie urządzeń służbowych do celów prywatnych;
30. przebywanie osób nieuprawnionych w pomieszczeniu przyjmowania interesantów;
31. przetwarzanie danych osobowych przez osobę, której nie zostało wydane upoważnienie do przetwarzania danych;
32. przechowywanie dokumentów zawierających dane osobowe po upływie okresu ich retencji;
33. utworzenie listy, na której zaznaczane są przyczyny nieobecności pracowników, w sposób umożliwiający innym pracownikom odczyt podanego powodu;
34. niewłaściwe niszczenie dokumentów umożliwiające odczyt „zniszczonych" danych osobowych np. poprzez używanie niszczarki paskowej zamiast ścinkowej;
35. ujawnienie dokumentacji wdrożeniowej RODO podmiotom nieuprawnionym;
36. posiadanie przez pracownika dostępu do zakresu danych osobowych niezgodnych z zajmowanym stanowiskiem, nie wydzielenie zakresów przetwarzania dla pracowników;
37. przekazywanie danych osobowych bez podpisanej umowy powierzenia lub bez podstawy prawnej;
38. udostępnienie zdjęć na stronie internetowej/portalach społecznościowych bez wcześniejszego uzyskania zgody;
39. wysłanie e-maila bez ukrycia adresów e-mail odbiorców (DW zamiast UDW).

Naruszenie należy niezwłocznie zgłosić przełożonemu, który wspólnie z Administratorem oraz Inspektorem Ochrony Danych (w przypadku jego wyznaczenia), podejmuje odpowiednie kroki w celu usunięcia bądź zminimalizowania skutków naruszenia.

**Załącznik nr 8**

**PRZYKŁADOWY WNIOSEK O REALIZACJĘ PRAW RODO**

.....
miejscowość i data

**Dane osoby wnioskującej:**
Imię/imiona: ……..

Nazwisko: ……..

Adres zamieszkania: ……..

……..

**Dane Administratora:**

Nazwa: ……..

Adres siedziby: …….

…….

***WNIOSEK O REALIZACJĘ***

Na podstawie art. 15-22 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 (ogólne rozporządzenie o ochronie danych) składam wniosek o realizację*:

□ prawa dostępu do danych
□ prawa do sprostowania danych
□ prawa do usunięcia danych ("prawo do bycia zapomnianym")
□ prawa do ograniczenia przetwarzania
□ prawa do przeniesienia danych do innego administratora
□ prawa do sprzeciwu
□ prawa do niepodlegania profilowaniu

**Uzasadnienie/uwagi osoby wnioskującej**

……
……

**Sposób odbioru danych osobowych przez osobę wnioskującą***

□ wiadomość e-mail: …….
□ doręczenie pocztą: ……..
□ odbiór osobisty

.....
*podpis wnioskodawcy*

**Decyzja administratora:**

□ Administrator przychyla się do wniosku
□ Administrator odrzuca wniosek

**Uzasadnienie decyzji administratora:**

……

……

.....
*data i podpis administratora*

* właściwe zaznaczyć