Art. 34. Zasada utylizacji sprzętu elektronicznego

1. W przypadku wycofania sprzętu elektronicznego z użycia, dane osobowe na nim zapisane powinny być kasowane przy użyciu przeznaczonego do tego oprogramowania do bezpiecznego usuwania danych, najlepiej za pomocą certyfikowanego urządzenia np. demagnetyzera.
2. W przypadku braku możliwości programowego usunięcia danych ze sprzętu elektronicznego podlega on fizycznemu zniszczeniu.
3. Zniszczenie sprzętu elektronicznego powinno być potwierdzane protokołem zniszczenia.

Rozdział IV
Inne środki organizacyjne i techniczne służące do zabezpieczania danych osobowych

Art. 35. Zasady bezpiecznej pracy

1. Każda osoba działająca z upoważnienia Administratora i mająca dostęp do danych, zobowiązana jest do stosowania następujących zasad bezpieczeństwa:
   1) **polityki „czystego biurka"** - w trakcie pracy na biurku powinny znajdować się tylko te materiały, które są niezbędne do wykonywania obowiązków służbowych. W przypadku opuszczenia stanowiska pracy przez osobę upoważnioną, materiały zawierające dane, wymagające szczególnej ochrony powinny być zabezpieczone przed dostępem osób nieuprawnionych. Po zakończeniu dnia pracy każda osoba zobowiązana jest do zabezpieczenia wszelkich dokumentów i nośników zawierających istotne dane, w celu uniemożliwienia dostępu do nich osobom nieuprawnionym;
   2) **polityki „czystego ekranu"** - w przypadku chwilowego opuszczenia stanowiska pracy każda osoba zobowiązana jest do wylogowania się z systemu, bądź zablokowania dostępu do pulpitu stacji roboczej w celu uniemożliwienia dostępu

do systemu operacyjnego lub aplikacji osobom nieuprawnionym. Ponadto w trakcie pracy należy mieć otwarte tylko te aplikacje, które są niezbędne do wykonywania obowiązków służbowych;

3) takiego ustawienia monitora, aby osoby niepowołane nie mogły zapoznać się z informacjami wyświetlanymi na monitorze. W przeciwnym wypadku należy wyposażyć monitor w odpowiedni filtr prywatyzujący;
4) bieżącego niszczenia w niszczarce niepotrzebnej dokumentacji papierowej oraz przechowywania pozostałej dokumentacji papierowej w zabezpieczonych szafach, zamykanych przynajmniej na klucz;
5) niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej;
6) zachowania w poufności wszelkich informacji, w tym danych osobowych poprzez złożenie stosownego oświadczenia;
7) niepozostawiania klucza w drzwiach biurowych po zewnętrznej stronie pomieszczenia;
8) niepozostawiania pomieszczeń biurowych bez opieki.

Art. 36. Zarządzanie ryzykiem

1. Administrator analizuje możliwe sytuacje i naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, zwane dalej „analizami ryzyka".
2. Administrator przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii.
3. Analiza ryzyka powinna zapewniać:
   1) zidentyfikowanie ryzyka;
   2) oszacowanie ryzyka z punktu widzenia następstw dla działalności Jednostki oraz

prawdopodobieństwa wystąpienia takiego ryzyka;

3) informowanie o następstwach wystąpienia ryzyka;
4) ustanowienie priorytetów w postępowaniu z ryzykiem;
5) regularne monitorowanie i przegląd różnych typów ryzyka oraz procesu zarządzania ryzykiem;
6) zbieranie informacji w celu doskonalenia podejścia do zarządzania ryzykiem.

4. Administrator dokumentuje wykonaną analizę ryzyka w postaci raportu.
5. Administrator dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych w przypadkach, w których zgodnie z analizą ryzyka, ryzyko naruszenia praw i wolności osób jest wysokie oraz w każdym przypadku, gdy wymagają tego obowiązujące przepisy prawa i wytyczne Prezesa Urzędu Ochrony Danych Osobowych.

Art. 37. Audyt wewnętrzny w zakresie bezpieczeństwa informacji

1. Administrator zapewnia przeprowadzenie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji nie rzadziej niż raz na rok lub częściej zgodnie z powszechnie obowiązującymi w tym zakresie przepisami.
2. Z przeprowadzonego audytu powinien zostać sporządzony raport.

Art. 38. Obszar przetwarzania i zarządzanie kluczami do pomieszczeń

1. Wszystkie pomieszczenia biurowe w Jednostce co do zasady stanowią obszar przetwarzania danych osobowych.
2. Dodatkowo Administrator określił szczególne obszary przetwarzania danych objęte dodatkowymi zabezpieczeniami, do których dostęp mają tylko osoby upoważnione przez Administratora.
3. Opis środków technicznych służących do zabezpieczenia danych osobowych oraz wskazanie obszaru przetwarzania zawiera **załącznik nr 15** do Polityki.

4. Administrator wyznaczył osoby, które są upoważnione do otwierania drzwi wejściowych do budynków Jednostki przed rozpoczęciem pracy Jednostki. Osoby, którym Administrator powierzył klucze zobowiązane są do nieudostępniania tych kluczy osobom trzecim.
5. Klucze do poszczególnych pomieszczeń posiadają osoby upoważnione, którym zostały wydane one na podstawie protokołów przekazania. Od momentu pobrania kluczy do momentu ich zdania na tych osobach spoczywa pełna odpowiedzialność za ich zabezpieczenie. Po otwarciu pomieszczeń biurowych, przed przystąpieniem do pracy, Użytkownicy sprawdzają stan zastosowanych zabezpieczeń.
6. Zapasowe klucze do wszystkich pomieszczeń Jednostki oraz klucze zapasowe do Bibliotek są odpowiednio zabezpieczone i przechowywane są w biurze Gminnego Ośrodka Kultury w Santoku. Każdorazowe użycie klucza zapasowego powinno być zgłoszone do Administratora.
7. Zabrania się pozostawiania kluczy do pomieszczeń z obszaru przetwarzania danych w drzwiach lub w miejscach ogólnie dostępnych, pomieszczenia te powinny być zamknięte na klucz na czas nieobecności osób upoważnionych w sposób uniemożliwiający dostęp do nich osobom trzecim.
8. Zabrania się dorabiania kluczy do pomieszczeń, szaf biurowych itp. bez zgody Administratora.
9. Zabrania się pozostawiania osób trzecich w pomieszczeniach biurowych Jednostki bez nadzoru osób upoważnionych przez Administratora.
10. Użytkownicy po godzinach pracy Jednostki mogą przebywać na obszarze przetwarzania danych osobowych jedynie za zgodą Administratora.
11. W przypadkach przebywania Użytkowników w pomieszczeniach obszaru przetwarzania danych po wyznaczonych godzinach pracy, godzinach pełnienia obowiązków, wykonywania zadań na rzecz Administratora należy upewnić się czy zamknięto drzwi wejściowe do obszaru przetwarzania danych osobowych. Dodatkowo opuszczając obszar przetwarzania danych należy sprawdzić czy zamknięto wszystkie okna oraz drzwi wejściowe do pomieszczeń.

12. Procedura regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania określona jest w **załączniku nr 16** do Polityki.

Art. 39. Ochrona danych osobowych w fazie projektowania i domyślna ochrona danych

1. Obowiązek uwzględnienia ochrony danych w fazie projektowania spoczywa na Administratorze. Administrator zobligowany jest do szczegółowej analizy i opisu planowanego procesu przetwarzania danych. Ponadto w przypadku, gdy do przetwarzania wykorzystywane będą narzędzia dostarczane Administratorowi przez zewnętrznych dostawców wymagane jest zaangażowanie tych podmiotów. W przypadku dostawcy będącego Podmiotem przetwarzającym uwzględnienia ochrony danych w fazie projektowania oparte jest na zasadach wynikających z art. 28 RODO.
2. Kluczowym wymogiem związanym z ochroną danych osobowych w fazie projektowania i domyślną ochroną danych jest niedopuszczenie do przetwarzania danych w sposób, który naruszałby poszczególne wymogi RODO poprzez:
   1) zebranie informacji o celach danego projektu oraz planowanych środkach realizacji tych celów;
   2) określenie adekwatnych - dla danego projektu – środków technicznych i organizacyjnych służących do ochrony danych osobowych;
   3) ocenę, czy z projektem łączą się ryzyka dla praw lub wolności i przyjęcie określonego mechanizmu postępowania z tym ryzykiem (ocena ryzyka może doprowadzić do konieczności przeprowadzenia pełnej oceny skutków a nawet uprzednich konsultacji z Prezesem Urzędu Ochrony Danych Osobowych);
   4) przypisanie ról w organizacji w zakresie dokonywania ww. ocen;
   5) przeszkolenie pracowników przed rozpoczęciem przetwarzania nowego projektu;
   6) planowanie terminów retencji danych;
   7) szczegółowe podstawy prawne podjęcia działań w danym procesie;
   8) zidentyfikowanie potencjalnych zagrożeń wewnętrznych i zewnętrznych;

9) wskazanie potencjalnych odbiorców danych.

3. Wymóg ochrony danych osobowych w fazie projektowania wymaga nie tylko oceny danego procesu przetwarzania danych przed jego rozpoczęciem, ale także monitorowania zgodności w czasie przetwarzania. Z punktu widzenia mechanizmu oceny nowych projektów i zarządzania projektami wprowadzono Rejestr czynności przetwarzania danych, który powinien podlegać bieżącym aktualizacjom.
4. Administrator zobowiązany jest do uwzględnienia procesu w stosownych upoważnieniach dla osób obsługujących proces.
5. Administrator zobowiązany jest do przedstawienia IOD ww. informacji w celu przeprowadzenia analizy ryzyka obejmującej nowy proces.

Rozdział V

Postanowienia końcowe

Art. 40. Przetwarzanie danych osobowych w celu prowadzenia postępowań rekrutacyjnych

1. Jednostka przetwarza dane osobowe kandydatów w związku z prowadzonym postępowaniem rekrutacyjnym w zakresie niezbędnym do jego przeprowadzenia. Na podstawie art. 13 ust. 1 i 2 RODO, Jednostka realizuje w stosunku do kandydatów obowiązek informacyjny.
2. Klauzula informacyjna jest zamieszczana w treści lub jako załącznik do ogłoszenia o naborze albo pracę. Każdorazowa zmiana treści klauzuli informacyjnej zawierającej informacje, o których mowa w art. 13 ust. 1 i 2 RODO, wymaga przeprowadzenia uprzednich konsultacji z IOD.
3. Jednostka, jako Administrator wdraża odpowiednie środki techniczne i organizacyjne mające na celu zapewnienie bezpieczeństwa danych osobowych kandydatów.

4. Jednostka jest zobowiązana podać do publicznej wiadomości wyniki naboru na wolne stanowisko pracy. Informacja podawana jest do publicznej wiadomości poprzez umieszczenie jej w widocznym miejscu w siedzibie Jednostki oraz w Biuletynie Informacji Publicznej.

Art. 41. Przekazywanie danych osobowych do państwa trzeciego lub organizacji międzynarodowych

1. Administrator lub osoba działająca w jego imieniu jest zobowiązany/-a poinformować IOD o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej.
2. W sytuacji, gdy dobór narzędzi do przetwarzania danych osobowych nastąpi w drodze wyłonienia najkorzystniejszej oferty w ramach postępowania o udzielenie zamówienia publicznego, IOD jest zawiadamiany o zamiarze przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej przez Administratora. Zawiadomienie IOD o zamiarze przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej powinno zawierać m. in. informację o nazwie państwa trzeciego lub organizacji międzynarodowej, informację o celu przekazania danych osobowych, a także informację o kategorii osób, których dane dotyczą oraz ich rodzaju. Zawiadomienie przekazywane jest na adres poczty elektronicznej IOD oraz obsługi prawnej Jednostki. Informacje zawarte w zawiadomieniu są niezbędne do zweryfikowania przez IOD oraz obsługę prawną Jednostki właściwej podstawy przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej.
3. Na podstawie ww. informacji, IOD dokonuje aktualizacji Rejestru czynności przetwarzania danych osobowych oraz właściwych klauzul informacyjnych, o ile przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej jest dopuszczalne w świetle rozdziału V RODO. W przypadku braku podstaw do przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej,

IOD oraz obsługa prawna Jednostki informuje Administratora o braku przesłanki legalizującej transfer danych osobowych.

Art. 42. E-usługi.

1. Administrator może wdrożyć i stosować narzędzia elektroniczne, środki komunikacji elektronicznej, inne środki łączności oraz usługi online w celu załatwiania spraw w kontaktach z podmiotami trzecimi m.in. na podstawie art. 14 KPA w zw. z w art. 20a ust. 1 albo 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2023 r. poz. 57 ze zm.) oraz w zw. z art. 2 pkt 5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344).
2. Przy wdrażaniu tego rodzaju systemów i narzędzi teleinformatycznych, Administrator ma obowiązek wydać stosowne polecenia i instrukcje w celu zapewnienia należytej ochrony danych osobowych przetwarzanych przez osoby upoważnione. Polecenia, instrukcje oraz zasady funkcjonowania systemu e-usług zostaną szczegółowo uregulowane w odrębnym dokumencie.

Art. 43. Informacje dotyczące Polityki ochrony danych osobowych

1. Każda osoba mająca dostęp do danych osobowych Jednostki jest zobowiązana zapoznać się z Polityką ochrony danych osobowych oraz potwierdzić ten fakt własnoręcznym podpisem na wykazie, którego wzór stanowi **załącznik nr 18** do Polityki.
2. Polityka winna podlegać przeglądom we współpracy z IOD i aktualizacji w przypadku zmian w otoczeniu organizacyjno-prawnym Administratora.
3. Dokument Polityki obowiązuje w wersji tradycyjnej (papierowej) i znajduje się w pomieszczeniu Administratora. Administrator udostępnia Politykę każdemu Użytkownikowi na jego żądanie.
4. Aktualizacja Polityki odbywać się będzie centralnie tj. w celu uniknięcia pomyłki co do obowiązującej w danym momencie wersji Polityki.

5. Przekazanie informacji o zmianach w Polityce powinno nastąpić poprzez zobowiązanie Użytkowników do zapoznania się w określonym czasie z treścią zaktualizowanej Polityki i podpisania przez nich ponownie wykazu osób zapoznanych z Polityką – **załącznik nr 18**.

Art. 44. Wykaz załączników

Załącznik nr 1 – Wzór oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych.
Załącznik nr 2 – Wzór oświadczenia o wycofaniu zgody na przetwarzanie danych osobowych.
Załącznik nr 3 – Wzór ogólnej klauzuli informacyjnej z art. 13 ust. 1 i 2.
Załącznik nr 4 – Wzór ogólnej klauzuli informacyjnej z art. 14 ust. 1 i 2.
Załącznik nr 5 – Procedura realizacji praw osób których dane dotyczą.
Załącznik nr 6 – Wzór upoważnienia do przetwarzania danych osobowych.
Załącznik nr 7 – Wzór oświadczenia o zachowaniu w tajemnicy danych osobowych.
Załącznik nr 8 – Ewidencja osób upoważnionych do przetwarzania danych osobowych.
Załącznik nr 9 – Informator dla Użytkowników z zakresu ochrony danych osobowych.
Załącznik nr 10 – Lista kontrolna Procesora.
Załącznik nr 11 – Wzór umowy powierzenia przetwarzania danych osobowych.
Załącznik nr 12 – Wzór rejestru zawartych umów powierzenia przetwarzania danych osobowych.
Załącznik nr 13- Procedura zarządzania naruszeniami ochrony danych osobowych
Załącznik nr 14 – Procedura użytkowania prywatnych urządzeń elektronicznych.
Załącznik nr 15 – Wzór opisu środków technicznych stosowanych do zabezpieczania danych osobowych i wykaz obszaru przetwarzania.
Załącznik nr 16 – Procedura regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
Załącznik nr 17- Procedury ochrony danych osobowych przy pracy zdalnej.
Załącznik nr 18 – Wykaz osób zapoznanych z Polityką ochrony danych osobowych.