Polityka ochrony danych osobowych w Gminnym Centrum Biblioteczno-Kulturalnym w Starych Bogaczowicach

Administrator danych osobowych:
Gminne Centrum Biblioteczno-Kulturalne w Starych Bogaczowicach, ul. Główna 148,
58-312 Stare Bogaczowice, REGON 890028986 tel. 74-8443503, e-mail: biblioteka@gcbk.pl.

Inspektor Ochrony Danych Osobowych:
Tomasz Rybiński
tel. 74-8443503 email: : iodo@gcbk.pl

POLITYKA OCHRONY DANYCH OSOBOWYCH

Niniejszy dokument zatytułowany „**Polityka ochrony danych osobowych**” (dalej jako **Polityka**) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w Gminnym Centrum Biblioteczno-Kulturalnym w Starych Bogaczowicach, ul. Główna 148, 58-312 Stare Bogaczowice, REGON 890028986 tel. 74-8443503, e-mail: biblioteka@gcbk.pl.
– (dalej jako **Instytucja kultury**).

Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (Dz.Urz. UE L 119, s. 1).

1. Polityka zawiera:

a) opis zasad ochrony danych obowiązujących w Instytucji kultury;

b) odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych są opisane w załącznikach);

2. Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest Administrator.

3. Za nadzór i monitorowanie przestrzegania Polityki odpowiada Inspektor Ochrony Danych.

4. Instytucja kultury powinna też zapewnić zgodność postępowania kontrahentów z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez Instytucję.

5. Skróty i definicje:

Polityka oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu.
RODO oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (Dz.Urz. UE L 119, s. 1).

Dane oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu.

Dane wrażliwe oznaczają dane specjalne i dane karne.

Dane specjalne oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

Dane karne oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa.

Dane dzieci oznaczają dane osób poniżej 16. roku życia.

Osoba oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.

Podmiot przetwarzający oznacza organizację lub osobę, której Instytucja kultury powierzyła przetwarzanie danych osobowych (np. usługodawca IT, zewnętrzna księgowość).

Profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Eksport danych oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej.

IOD lub Inspektor oznacza Inspektora Ochrony Danych Osobowych

RCPD lub Rejestr oznacza Rejestr Czynności Przetwarzania Danych Osobowych.

Instytucja kultury oznacza Centrum Kultury w Jedlinie-Zdroju ul. Piastowska 13, 58-330 Jedlina-Zdrój

Ochrona danych osobowych w Instytucji kultury – zasady ogólne

5.1. Filary ochrony danych osobowych w Instytucji kultury:

(1) **Legalność** − Instytucja kultury dba o ochronę prywatności i przetwarza dane zgodnie z prawem.

(2) **Bezpieczeństwo** − Instytucja kultury zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.

(3) **Prawa Jednostki** − Instytucja kultury umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.

(4) **Rozliczalność** − Instytucja kultury dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

5.2. Zasady ochrony danych

Instytucja kultury przetwarza dane osobowe z poszanowaniem następujących zasad:

(1) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);

(2) rzetelnie i uczciwie (rzetelność);

(3) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);

(4) w konkretnych celach i nie „na zapas" (minimalizacja);

(5) nie więcej niż potrzeba (adekwatność);

(6) z dbałością o prawidłowość danych (prawidłowość);

(7) nie dłużej niż potrzeba (czasowość);

(8) zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

5.3. System ochrony danych

System ochrony danych osobowych w Instytucji kultury składa się z następujących elementów:

1) **Inwentaryzacja danych.** Instytucja kultury dokonuje identyfikacji zasobów danych osobowych w Instytucji kultury, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych (inwentaryzacja), w tym:

a) przypadków przetwarzania danych specjalnych i danych „kryminalnych" (**dane wrażliwe**);

b) przypadków przetwarzania danych osób, których Instytucja kultury nie identyfikuje (**dane niezidentyfikowane**);

c) przypadków przetwarzania danych dzieci;

d) profilowania;

e) współadministrowania danymi.

2) **Rejestr.** Instytucja kultury opracowuje, prowadzi i utrzymuje Rejestr Czynności Danych Osobowych w Instytucji kultury (Rejestr). Rejestr jest narzędziem rozliczania zgodności z ochroną danych w Instytucji kultury.

3) **Podstawy prawne.** Instytucja kultury zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:

a) utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikację na odległość,

b) inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy Instytucja kultury przetwarza dane na podstawie prawnie uzasadnionego interesu Instytucji kultury.

4) **Obsługa praw jednostki.** Instytucja kultury spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:

a) **Obowiązki informacyjne.** Instytucja kultury przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków.

b) **Możliwość wykonania żądań.** Instytucja kultury weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających.

c) **Obsługa żądań.** Instytucja kultury zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO i dokumentowane.

d) **Zawiadamianie o naruszeniach.** Instytucja kultury stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

5) **Minimalizacja.** Instytucja kultury posiada zasady i metody zarządzania minimalizacją (*privacy by default*), a w tym:

a) zasady zarządzania **adekwatnością** danych;

b) zasady reglamentacji i zarządzania **dostępem** do danych;

c) zasady zarządzania okresem **przechowywania** danych i weryfikacji dalszej przydatności;

6) **Bezpieczeństwo.** Instytucja kultury zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:

a) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;

b) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;

c) dostosowuje środki ochrony danych do ustalonego ryzyka;

d) posiada system zarządzania bezpieczeństwem informacji;

e) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych − zarządza incydentami.

7) **Przetwarzający.** Instytucja kultury posiada zasady doboru przetwarzających dane na rzecz Instytucji kultury, wymogów co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia.

8) **Eksport danych.** Instytucja kultury posiada zasady weryfikacji, czy Instytucja kultury nie przekazuje danych do państw trzecich (czyli poza UE, Norwegię, Lichtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków takiego przekazywania, jeśli ma ono miejsce.

9) ***Privacy by design*.** Instytucja kultury zarządza zmianami mającymi wpływ na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji w Instytucji kultury uwzględniają konieczność oceny wpływu zmiany na ochronę danych, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.

10) Przetwarzanie transgraniczne. Instytucja kultury posiada zasady weryfikacji, kiedy zachodzą przypadki przetwarzania transgranicznego oraz zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO.

6. Inwentaryzacja

6.1. Dane wrażliwe

Instytucja kultury identyfikuje przypadki, w których przetwarza lub może przetwarzać dane wrażliwe (dane specjalne i dane karne) oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania danych wrażliwych. W przypadku zidentyfikowania przypadków przetwarzania danych wrażliwych, Instytucja kultury postępuje zgodnie z przyjętymi zasadami w tym zakresie.

6.2. Dane niezidentyfikowane

Instytucja kultury identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane.

6.3. Współadministrowanie

Instytucja kultury identyfikuje przypadki współadministrowania danymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami.

7. Rejestr Czynności Przetwarzania Danych

7.1. RCPD stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.

7.2. Instytucja kultury prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.

7.3. Rejestr jest jednym z podstawowych narzędzi umożliwiających Instytucji kultury rozliczanie większości obowiązków ochrony danych.

7.4. W Rejestrze, dla każdej czynności przetwarzania danych, którą Instytucja kultury uznała za odrębną dla potrzeb Rejestru, Instytucja kultury odnotowuje co najmniej:

- nazwę czynności,
- cel przetwarzania,
- opis kategorii osób,
- opis kategorii danych,

- podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu Instytucji kultury, jeśli podstawą jest uzasadniony interes,
- sposób zbierania danych,
- opis kategorii odbiorców danych (w tym przetwarzających),
- informację o przekazaniu poza EU/EOG;
- ogólny opis technicznych i organizacyjnych środków ochrony danych.

7.5. Wzór Rejestru stanowi **Załącznik nr 1 do Polityki – „Wzór Rejestru Czynności Przetwarzania Danych".** Wzór Rejestru zawiera także kolumny nieobowiązkowe. W kolumnach nieobowiązkowych Instytucja kultury rejestruje informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść Rejestru ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej

6. Podstawy przetwarzania

8.1. Instytucja kultury dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.

8.2. Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel Instytucji kultury) Instytucja kultury dookreśla podstawę w czytelny sposób, gdy jest to potrzebne. Np. dla zgody wskazując na jej zakres, gdy podstawą jest prawo – wskazując na konkretny przepis i inne dokumenty, np. umowę, porozumienie administracyjne, żywotne interesy – wskazując na kategorie zdarzeń, w których się zmaterializują, uzasadniony cel – wskazując na konkretny cel, np. dochodzenie roszczeń.

8.3. Instytucja kultury wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (email) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).

8.4. Kierownik komórki organizacyjnej Instytucji kultury ma obowiązek znać podstawy prawne, na jakich komórka przez niego kierowana dokonuje konkretnych czynności przetwarzania danych osobowych. Jeżeli podstawą jest uzasadniony interes Instytucji kultury, kierownik komórki ma obowiązek znać konkretny realizowany przetwarzaniem interes Instytucji kultury.

9. Sposób obsługi praw jednostki i obowiązków informacyjnych

9.1. Instytucja kultury dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.

9.2. Instytucja kultury ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczenie na stronie internetowej Instytucji kultury informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich w Instytucji kultury.

9.3. Instytucja kultury dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.

9.4. Instytucja kultury wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.

9.5. W celu realizacji praw jednostki Instytucja kultury zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Instytucję, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany.

9.6. Instytucja kultury dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

10. Obowiązki informacyjne

10.1. Instytucja kultury określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.

10.2. Instytucja kultury informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.

10.3. Instytucja kultury informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.

10.4. Instytucja kultury określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym).

10.5. Instytucja kultury informuje osobę o planowanej zmianie celu przetwarzania danych.

10.6. Instytucja kultury informuje osobę przed uchyleniem ograniczenia przetwarzania.

10.7. Instytucja kultury informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).

10.8. Instytucja kultury informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.

10.9. Instytucja kultury bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

Zgodnie z wzorami klauzul informacyjnych które stanowią **Załącznik nr 9 do Polityki**

11. Żądania osób

11.1. **Prawa osób trzecich**. Realizując prawa osób, których dane dotyczą, Instytucja kultury wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnicę handlową, dobra osobiste itp.), Instytucja kultury może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

11.2. **Nieprzetwarzanie**. Instytucja kultury informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.

11.3. **Odmowa**. Instytucja kultury informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.

11.4. **Dostęp do danych**. Na żądanie osoby dotyczące dostępu do jej danych, Instytucja kultury informuje osobę, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych, z zastrzeżeniem, że kopii danych wydanej w wykonaniu prawa dostępu do danych Instytucja kultury nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.

11.5. **Kopie danych**. Na żądanie Instytucja kultury wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Instytucja kultury wprowadza i utrzymuje cennik kopii danych, zgodnie z którym pobiera opłaty za kolejne

kopie danych. Cena kopii danych skalkulowana jest w oparciu o oszacowany jednostkowy koszt obsługi żądania wydania kopii danych.

11.6. Sprostowanie danych. Instytucja kultury dokonuje sprostowania nieprawidłowych danych na żądanie osoby. Instytucja kultury ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Instytucja kultury informuje osobę o odbiorcach danych, na żądanie tej osoby.

11.7. Uzupełnienie danych. Instytucja kultury uzupełnia i aktualizuje dane na żądanie osoby. Instytucja kultury ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. Instytucja kultury nie musi przetwarzać danych, które są Instytucji kultury zbędne). Instytucja kultury może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Instytucję procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

11.8. Usunięcie danych. Na żądanie osoby, Instytucja kultury usuwa dane, gdy:

a) dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,

b) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,

c) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,

d) dane były przetwarzane niezgodnie z prawem,

e) konieczność usunięcia wynika z obowiązku prawnego,

f) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. profil dziecka na portalu społecznościowym, udział w konkursie na stronie internetowej).

Instytucja kultury określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17. ust. 3 RODO.

Jeżeli dane podlegające usunięciu zostały upublicznione przez Instytucję, Instytucja kultury podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych

administratorów przetwarzających te dane osobowe, o potrzebie usunięcia danych i dostępu do nich.
W przypadku usunięcia danych Instytucja kultury informuje osobę o odbiorcach danych, na żądanie tej osoby.

11.9. Ograniczenie przetwarzania. Instytucja kultury dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:

a) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,

b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,

c) Instytucja kultury nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,

d) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Instytucji kultury zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

W trakcie ograniczenia przetwarzania Instytucja kultury przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.
Instytucja kultury informuje osobę przed uchyleniem ograniczenia przetwarzania.
W przypadku ograniczenia przetwarzania danych Instytucja kultury informuje osobę o odbiorcach danych, na żądanie tej osoby.

11.10. Przenoszenie danych. Na żądanie osoby Instytucja kultury wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, **jeśli** jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Instytucji kultury, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Instytucji kultury.

11.11. Sprzeciw w szczególnej sytuacji. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Instytucję w oparciu o uzasadniony interes Instytucji kultury lub o powierzone Instytucji kultury zadanie w interesie publicznym, Instytucja kultury **uwzględni** sprzeciw, o ile nie zachodzą po stronie Instytucji kultury ważne prawnie uzasadnione podstawy do

przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

11.12. Sprzeciw przy badaniach naukowych, historycznych lub celach statystycznych. Jeżeli Instytucja kultury prowadzi badania naukowe, historyczne lub przetwarza dane w celach statystycznych, osoba może **wnieść** umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania. Instytucja kultury uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

12. MINIMALIZACJA

Instytucja kultury dba o minimalizację przetwarzania danych pod kątem:

a) adekwatności danych do celów (ilości danych i zakresu **przetwarzania**),
b) dostępu do danych,
c) czasu przechowywania danych.

12.1. Minimalizacja zakresu

Instytucja kultury zweryfikowała zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO.
Instytucja kultury dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.
Instytucja kultury przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (*privacy by design*).

12.2. Minimalizacja dostępu

Instytucja kultury stosuje ograniczenia dostępu do danych osobowych: prawne (zobowiązania do poufności, zakresy upoważnień), fizyczne (strefy dostępu, zamykanie pomieszczeń) i logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe).
Instytucja kultury stosuje kontrolę dostępu fizycznego.
Instytucja kultury dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających.
Instytucja kultury dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.
Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w procedurach bezpieczeństwa fizycznego i bezpieczeństwa informacji Instytucji kultury.

12.3. Minimalizacja czasu

Instytucja kultury wdraża mechanizmy kontroli cyklu życia danych osobowych w Instytucji kultury, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze.

Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów produkcyjnych Instytucji kultury, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Instytucję. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

13. BEZPIECZEŃSTWO

Instytucja kultury zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Spółkę.

13.1. Analizy ryzyka i adekwatności środków bezpieczeństwa

Instytucja kultury przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:

a) Instytucja kultury zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania − wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.

b) Instytucja kultury kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.

c) Instytucja kultury przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Instytucja kultury analizuje możliwe sytuacje i scenariusze 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.

d) Instytucja kultury ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym Instytucja kultury ustala przydatność i stosuje takie środki i podejście jak:

- pseudonimizacja,
- szyfrowanie danych osobowych,

- inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,

- środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

13.2. Oceny skutków dla ochrony danych

Instytucja kultury dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.
Instytucja kultury stosuje metodykę oceny skutków przyjętą w Instytucji kultury.

13.3. Środki bezpieczeństwa

Instytucja kultury dla zapewnienia bezpieczeństwa stosuje środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych bliżej opisane w procedurach stanowiący Załącznik nr 4 przyjętych przez Instytucję.

13.4. Zgłaszanie naruszeń

Instytucja kultury stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia.

14. PRZETWARZAJĄCY

Instytucja kultury posiada zasady doboru i weryfikacji przetwarzających dane na rzecz Instytucji kultury opracowane w celu zapewnienia, aby przetwarzający dawali wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na Instytucji kultury.

Instytucja kultury przyjęła minimalne wymagania co do umowy powierzenia przetwarzania danych stanowiące **Załącznik nr 2 do Polityki – „Wzór umowy powierzenia przetwarzania danych”** po podpisaniu załącznika **Załącznik nr 8 do Polityki – „Zgoda na podpowierzenie”**

Instytucja kultury rozlicza przetwarzających z wykorzystania podprzetwarzających, jak też z innych wymagań wynikających z Zasad powierzenia danych osobowych.

15. PROJEKTOWANIE PRYWATNOŚCI

Instytucja kultury 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 Instytucję 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.

16. POSTANOWIENIA KOŃCOWE

Polityka jest dokumentem wewnętrznym i nie może być udostępniania osobom nieupoważnionym w żadnej formie.

a) Każda osoba przetwarzająca dane osobowe zobowiązana jest do zapoznania się z treścią Polityki Ochrony Danych.
b) Użytkownik zobowiązany jest złożyć oświadczenie, o tym, że został zaznajomiony z przepisami ustawy o ochronie danych osobowych, wydanymi na jej podstawie aktami wykonawczymi, obowiązującą Polityką.
c) Oświadczenia przechowywane są w aktach personalnych pracownika.
d) W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy RODO oraz wydanych na jej podstawie aktów wykonawczych.
e) Użytkownicy zobowiązani są do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce.

Załącznik nr 1 do Polityki ochrony danych osobowych

Wzór rejestru czynności przetwarzania danych osobowych

Rejestr czynności przetwarzania danych osobowych	
Nazwa administratora danych lub podmiotu przetwarzającego / przedstawiciela administratora lub podmiotu przetwarzającego	
Współadministratorzy	
Inspektor ochrony danych	
Cel przetwarzania	
Opis kategorii osób	
Kategorie odbiorców	
Kategorie danych osobowych	
Informacje o przekazaniu do państwa trzeciego lub organizacji międzynarodowej	
Planowany termin usunięcia danych osobowych	
Opis technicznych i organizacyjnych środków bezpieczeństwa	

Załącznik nr 2 do Polityki ochrony danych osobowych

Wzór umowy powierzenia przetwarzania danych osobowych

Umowa powierzenia przetwarzania danych osobowych

zawarta w ……., ... pomiędzy:

XYZ sp. z o.o. …….,

zwaną dalej Zleceniodawcą lub Administratorem

a

…….,

zwaną dalej Zleceniobiorcą lub Podmiotem przetwarzającym

zwanymi każdą z osobna w dalszej części Umowy „Stroną", a łącznie „Stronami".

Zważywszy, że:

- Zleceniobiorca będzie wykonywał odpłatne świadczenie na rzecz Zleceniodawcy usług z zakresu obsługi …….,
- Zleceniobiorca w ramach usług będzie miał dostęp do danych osobowych pracowników Administratora,

Strony niniejszym postanawiają zawrzeć Umowę powierzenia przetwarzania danych osobowych („Umowa"), o następującej treści:

§ 1

Oświadczenia Stron

1. Administrator powierza Zleceniobiorcy do przetwarzania dane osobowe, które zgromadził zgodnie z obowiązującymi przepisami prawa i przetwarza w zbiorze danych o nazwie ……

2. Zleceniobiorca oświadcza, że dysponuje środkami umożliwiającymi prawidłowe przetwarzanie danych osobowych powierzonych przez Administratora, w zakresie i celu określonym Umową.

3. Zleceniobiorca oświadcza również, że osobom zatrudnionym przy przetwarzaniu powierzonych danych osobowych nadane zostały upoważnienia do przetwarzania danych osobowych oraz że osoby te zostały zapoznane z przepisami o ochronie danych osobowych oraz z odpowiedzialnością za ich nieprzestrzeganie, zobowiązały się do ich przestrzegania oraz do bezterminowego zachowania w tajemnicy przetwarzanych danych osobowych i sposobów ich zabezpieczenia.

§ 2

Cel, zakres, miejsce przetwarzania powierzonych danych osobowych

1. Administrator powierza Zleceniobiorcy przetwarzanie danych osobowych …… jedynie w celu prawidłowego wykonywania usługi ……
2. Zleceniobiorca zobowiązuje się do przetwarzania powierzonych danych osobowych wyłącznie w celach związanych z realizacją Umowy i wyłącznie w zakresie, jaki jest niezbędny do realizacji tych celów.
3. Na wniosek Administratora lub osoby, której dane dotyczą, Zleceniobiorca wskaże miejsca, w których przetwarza powierzone dane.

§ 3

Zasady przetwarzania danych osobowych

1. Strony zobowiązują się wykonywać zobowiązania wynikające z niniejszej Umowy z najwyższą starannością zawodową w celu zabezpieczenia prawnego, organizacyjnego i technicznego interesów Stron w zakresie przetwarzania powierzonych danych osobowych.
2. Zleceniobiorca zobowiązuje się zastosować środki techniczne i organizacyjne mające na celu należyte, odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, zabezpieczenie powierzonych do przetwarzania danych osobowych, w szczególności zabezpieczyć je przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
3. Zleceniobiorca oświadcza, że zastosowane do przetwarzania powierzonych danych systemy informatyczne spełniają wymogi aktualnie obowiązujących przepisów prawa.
4. Zleceniobiorca przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora.
5. Podmiot przetwarzający, biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw.
6. Podmiot przetwarzający, uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga Administratorowi wywiązać się z obowiązków określonych w art. 32–36 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych).
7. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji Administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że szczególne przepisy prawa nakazują przechowywanie danych osobowych.

8. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszej umowie oraz umożliwia Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

5. Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody Administratora.

§ 4

Odpowiedzialność Stron

1. Administrator ponosi odpowiedzialność za przestrzeganie przepisów prawa w zakresie przetwarzania i ochrony danych osobowych według rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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. Powyższe nie wyłącza odpowiedzialności Zleceniobiorcy za przetwarzanie powierzonych danych niezgodnie z umową.

3. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem, jeśli nie dopełnił obowiązków, które nakłada na niego niniejsza umowa, lub gdy działał poza zgodnymi z prawem instrukcjami Administratora lub wbrew tym instrukcjom.

§ 5

Postanowienia końcowe

1. Wszelkie zmiany niniejszej Umowy powinny być dokonane w formie pisemnej pod rygorem nieważności.

2. W zakresie nieuregulowanym niniejszą Umową zastosowanie mają przepisy Kodeksu cywilnego.

3. W przypadku gdy niniejsza Umowa odwołuje się do przepisów prawa, oznacza to również inne przepisy dotyczące ochrony danych osobowych, a także wszelkie nowelizacje, jakie wejdą w życie po dniu zawarcia Umowy, jak również akty prawne, które zastąpią wskazane ustawy i rozporządzenia.

4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

5. Niniejsza umowa powierzenia przetwarzania danych osobowych obowiązuje na czas trwania umowy na świadczenie przez Zleceniobiorcę na rzecz Zleceniodawcy usług z zakresu ……

……..	……..
Zleceniodawca	Zleceniobiorca

Załącznik 3 do polityki ochrony danych osobowych

Protokół zniszczenia zbioru danych osobowych

Data operacji:……..…

Nazwa zbioru danych osobowych:……

Oznaczenie niszczonej kopii zapasowej:…….…...……/……..……

Rodzaj nośnika z kopią zapasową…….

Sposób zniszczenia:…….…..

Protokół sporządził:

Imię:……...……

Nazwisko:……..

.....	.....
data i podpis osoby sporządzającej protokół	data i podpis Inspektora Ochrony Danych Osobowych

* Niepotrzebne skreślić

Załącznik nr 4

Procedury postępowania przy przetwarzaniu danych osobowych:

1) Procedura określająca sposób postępowania z danymi osobowymi w formie papierowej i elektronicznej.

2) Procedura nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym

3) Procedura metod i środków uwierzytelnienia

4) Procedura rozpoczęcia pracy systemu informatycznego przeznaczona dla użytkowników systemu.

5) Procedura zawieszenia pracy systemu informatycznego przeznaczona dla użytkowników systemu.

6) Procedura zakończenia pracy systemu informatycznego przeznaczona dla użytkowników systemu.

7) Procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

8) Procedura bezpiecznego korzystania z poczty elektronicznej i postępowania użytkownika na okoliczność zidentyfikowania określonego typu zagrożeń przez program antywirusowy

9) Procedura wykonywania przeglądów i konserwacji systemów.

10) Procedura wykonywania przeglądów i konserwacji nośników informacji służących do przetwarzania danych.

11) Procedura postępowania w sytuacji naruszenia ochrony danych osobowych.

12) Procedura niszczenia zbiorów zawierających dane osobowe

13) Procedura postępowanie w wypadku klęski żywiołowej.

14) Procedura użytkowania komputerów przenośnych

15) Procedura kontroli przestrzegania zasad zabezpieczenia ochrony danych osobowych

Procedura organizacyjna postępowania pracownika z danymi osobowymi w formie papierowej i elektronicznej.	
numer procedury: 1	
dotyczy:	wszystkich użytkowników przetwarzających dane osobowe

1. Przed przystąpieniem do przetwarzania danych pracownik zapoznaje się z przepisami dotyczącymi ochrony osobowych, w tym celu osoba jest kierowana do Inspektora Ochrony Danych Osobowych celem zapoznania z przepisami o Ochronie Danych Osobowych oraz dokumentami wewnętrznymi w tym zakresie. Oświadczenie o zaznajomieniu z przepisami, po podpisaniu, trafia do dokumentacji kadrowej danej osoby.
2. Pracownik ma obowiązek kontrolowania pomieszczeń, w których są przetwarzane dane osobowe tak aby osoby nieupoważnione nie maiły do niego dostępu.
3. Pracownik po zakończeniu pracy dokumenty przechowuje się w szafach zamkniętych na klucz.
4. Wszystkich pracowników obowiązuje polityka czystego biurka i czystego ekranu. **Polityka czystego biurka** oznacza chowanie do szaf dokumentów po zakończeniu pracy. Żadne dokumenty nie zostają po godzinach pracy na biurkach. **Polityka czystego ekranu** oznacza stosowanie środków uniemożliwiających wgląd osobom trzecim do informacji przetwarzanych na ekranie komputera.
5. Wszystkie dokumenty niepotrzebne muszą być niszczone w sposób nie pozwalający na odtworzenie zawartych w nich informacji, np. w niszczarkach dokumentów
6. Po każdej aktualizacji w/w dokumentacji organizowane są szkolenia celem zaznajomienia pracowników ze zmianami.
7. pomieszczenia, w których są przetwarzane dane osobowe, zamyka się na czas nieobecności pracowników.
8. Na stanowiskach pracy należy dbać, by po zakończeniu pracy wszystkie dokumenty były chowane do szaf zamykanych na klucz.
9. Klucze od szaf przechowywane są w metalowej kasetce w wyznaczonym miejscu.
10. Klucze do pomieszczeń podlegają szczególnej ochronie.
11. Zabrania się umożliwianiu osób nieupoważnionych do danych osobowych, w tym do systemów informatycznych.
12. Dla nowo zatrudnionego pracownika stosuje się następujące zasady:

- Pracownik odbywa szkolenie u Inspektora Ochrony Danych Osobowych polegające na zapoznaniu się z przepisami o Ochronie Danych osobowych i Polityką Ochrony Danych Osobowych funkcjonującą w organizacji.

Na szkolenie kieruje pracownik ds. Kadr.

- Po szkoleniu pracownik potwierdza odbycie szkolenia własnoręcznym podpisem na oświadczeniu. Oświadczenie trafia do akt osobowych osoby zatrudnionej przy przetwarzaniu danych osobowych
- Pracownik otrzymuje upoważnienie do przetwarzania danych osobowych oraz zostaje zobowiązany do przestrzegania zasad dot. ochrony danych
- Inspektor Ochrony Danych Osobowych prowadzi ewidencję upoważnień.

Procedura nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym	
numer procedury: 2	
dotyczy:	wszystkich użytkowników systemów informatycznych

1. Rejestrowanie użytkownika i nadawanie uprawnień przeprowadza osobiście Administrator systemu, na podstawie upoważnienia do przetwarzania danych osobowych
2. Rejestrowanie użytkownika i nadawanie uprawnień wprowadzane się zgodnie z procedurami obsługi danego systemu informatycznego w zakresie niezbędnym do realizacji obowiązków służbowych.
3. Hasła użytkowników uprzywilejowanych (administratora) przechowywane są we wskazanym miejscu w zaplombowanych kopertach oddzielnie.
4. Użytkowników uprzywilejowanych rejestruje w systemie informatycznym dostawca oprogramowania, chyba że użytkownik uprzywilejowany jest kontem wbudowanym w systemie (admin, administrator).
5. W przypadku nieobecności administratora, w razie konieczności, można użyć hasła do konta administracyjnego.

Procedura metod i środków uwierzytelnienia	
numer procedury: 3	
dotyczy:	wszystkich użytkowników systemów informatycznych
osoby odpowiedzialne:	wszyscy użytkownicy systemów informatycznych

1. W systemie, służącym do przetwarzania danych osobowych, stosowane jest uwierzytelnianie użytkownika przy pomocy jego identyfikatora i hasła.
2. Użytkowników systemu obowiązuje następująca polityka haseł:
a) minimalna długość hasła wynosi 8 (osiem) znaków,
b) zmiana hasła nie rzadziej niż co 30 dni,
c) hasło zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
3. Każdy użytkownik systemu posiada swój unikalny identyfikator. Nazwa użytkownika (login) jest przydzielana pracownikowi odgórnie podczas upoważnienia pracownika do przetwarzania danych osobowych. Login składa się z liter i kojarzy się z imieniem i nazwiskiem użytkownika typu [pierwsza litera imienia][nazwisko],
4. Użytkownicy systemu nie mogą używać tych samych identyfikatorów, ani wymieniać się identyfikatorami. Użytkownik chroni hasło przed osobami postronnymi
5. Każdy użytkownik zarządza swoimi hasłami oraz utrzymuje hasła w tajemnicy.
6. System informatyczny winien pamiętać historię ostatnich haseł by nie pozwolić na użytkowanie tego samego hasła cały czas.
7. Hasła w systemie informatycznym powinny być przechowywane w postaci zaszyfrowanej.
8. Administrator systemu nadaje pierwszy raz hasło oraz zaznajamia użytkownika z obsługą mechanizmu uwierzytelniania oraz zmiany hasła.
9. Pierwsze hasło przekazywane jest użytkownikowi ustnie.
10. Użytkownik po otrzymaniu hasła jest zobowiązany do niezwłocznej jego zmiany, chyba, że system nie umożliwia wykonania takiej operacji.

Procedura rozpoczęcia pracy systemu informatycznego przeznaczona dla użytkowników systemu	
numer procedury: 4	
dotyczy:	wszystkich użytkowników systemów informatycznych
osoby odpowiedzialne:	wszyscy użytkownicy systemów informatycznych

1. Przed przystąpieniem do pracy należy sprawdzić stanowisko pracy.
2. Włączyć zasilanie stanowiska zgodnie z instrukcją obsługi zasilacza UPS.
3. Włączyć komputer.
4. Dokonać uwierzytelnienia zgodnie z monitem systemu operacyjnego komputera.
5. Bezwzględnie należy zapewnić zachowanie poufności podczas wprowadzania hasła.
6. Po uruchomieniu sytemu operacyjnego można rozpocząć pracę na programie użytkowym.
7. W razie problemów związanych z uruchamianiem systemu lub uwierzytelnianiem, lub stwierdzeniem fizycznej ingerencji w przetwarzane dane, należy się skontaktować z administratorem systemu i Inspektorem Ochrony Danych Osobowych.

Procedura zawieszenia pracy systemu informatycznego przeznaczona dla użytkowników systemu	
numer procedury: 5	
dotyczy:	wszystkich użytkowników systemów informatycznych
osoby odpowiedzialne:	wszyscy użytkownicy systemów informatycznych

1. Podczas nawet chwilowego opuszczenia stanowiska pracy należy zablokować możliwość wglądu do przetwarzanych danych przez osoby postronne poprzez zablokowanie stacji używając klawiszy **[Windows] + L** lub wylogowanie użytkownika z aplikacji / systemu operacyjnego.
2. Na czas dłuższej nieobecności zalecane jest wyłączenie stanowiska komputerowego.

Procedura zakończenia pracy systemu informatycznego przeznaczona dla użytkowników systemu	
numer procedury: 6	
dotyczy:	wszystkich użytkowników systemów informatycznych
osoby odpowiedzialne:	wszyscy użytkownicy systemów informatycznych

1. Wyrejestrować się z aplikacji użytkowej używając do tego odpowiedniej opcji.
2. Dokonać zamknięcia sytemu operacyjnego odpowiednią funkcją.
3. Odczekać aż system operacyjny zostanie wyłączony
4. Wyłączyć zasilanie stanowiska komputerowego poprzez wyłączenie zasilacza UPS zgodnie z instrukcją obsługi zasilacza.
5. W razie problemów związanych z zamykaniem systemu informatycznego należy się skontaktować z administratorem systemu.

Procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania	
numer procedury: 7	
dotyczy:	wszystkich użytkowników systemów informatycznych

1. Konfiguracja programów użytkowych powinna zapewniać przechowywanie zbiorów danych na wydzielonym zasobie serwera.
2. Serwer zapewnia automatyczną całościową archiwizację danych w cyklu codziennym lub z odstępem parudniowym w zależności od częstości wprowadzania danych.
3. Czasookres przechowywania kopii zapasowych na zasobach pamięci dyskowej wynosi nie mniej niż pół roku.
4. Każda kopia jest zachowywana z odnotowaniem daty i godziny powstania jako części jej nazwy
5. Do utworzenia kopii używane są narzędzia przewidziane w serwerach baz danych (SQL Serwer) oraz program do archiwizacji.
6. Nad poprawnością funkcjonowania systemu archiwizacji czuwa administrator systemu informatycznego
7. Kopie awaryjne tworzone doraźnie należy usuwać bezzwłocznie po ustaniu ich użyteczności.
8. Szczegółowy opis tworzenia kopii danych jest opisany w logach systemu".

Procedura bezpiecznego korzystania z poczty elektronicznej i postępowania użytkownika na okoliczność zidentyfikowania określonego typu zagrożeń przez program antywirusowy	
numer procedury: 8	
dotyczy:	wszystkich użytkowników systemów informatycznych
osoby odpowiedzialne:	wszyscy użytkownicy systemów informatycznych

1. Przeglądając wiadomości w skrzynce e-mail, przed przystąpieniem od otwierania załącznika lub linku z treści maila należy odpowiedzieć na kilka pytań, jest to pomoc w identyfikacji niebezpiecznych e-maili.

   - Czy znasz nadawcę wiadomości?
   - Czy otrzymywałeś już inne wiadomości od tego nadawcy?
   - Czy spodziewałeś się otrzymać tę wiadomość?
   - Czy tytuł wiadomości i nazwa załącznika mają sens?
   - Czy wiadomość nie zawiera złośliwego oprogramowania – jaki jest wynik skanowania antywirusowego?

   Ważne Negatywna odpowiedz na którekolwiek w/w pytanie powinny uruchomić procedurę informowania o próbie naruszenia danych.

2. Użytkownik powinien zapoznać się z obsługą systemu antywirusowego dostępną w formie podręcznika pod adresem:
https://www.eset.pl/resources/documents/HE-v10/eset_eav_10_userguide_plk.pdf

3. Po odebraniu zainfekowanej wiadomości e-mail, wykrycia zagrożenia na nośniku lub zagrożenia pochodzącego ze strony sieci internet system antywirusowy podejmuje działanie usuwając zagrożenie. W przypadku monitu o podjęcie działania zaleca się wybór opcji **Wylecz, Usuń** lub **Rozłącz**.

Procedura wykonywania przeglądów i konserwacji systemów	
numer procedury: 9	
dotyczy:	wszystkich użytkowników systemów informatycznych

1. Przeglądu oraz konserwacji systemów informatycznych dokonuje się raz na rok.
2. Przegląd obejmuje sprawdzenie stanu pamięci dyskowej, rejestru komunikatów systemowych (jeśli takie są w systemie operacyjnym komputera), sprawdzenie konfiguracji systemu.
3. Konserwacja obejmuje: czyszczenie z kurzu, sprawdzenie napięć wyjściowych z zasilacza. Ocena stanu systemu chłodzenia, wymianę wadliwych elementów, oraz usunięcie błędów logicznych.
4. Każda usterka jest natychmiast usuwana osobiście przez administratora systemu informatycznego. Podzespoły lub części nie zawierające danych osobowych mogą być przekazywane do naprawy podmiotom zewnętrznym.
5. W razie niestabilności systemu informatycznego dokonuje się przeglądu doraźnego.

Procedura wykonywania przeglądów i konserwacji nośników informacji służących do przetwarzania danych	
numer procedury: 10	
dotyczy:	wszystkich użytkowników systemów informatycznych
osoby odpowiedzialne:	wszystkich użytkowników systemów informatycznych

1. Nośniki informacji służące do przetwarzania danych takie jak twarde dyski, płyty CD podlegają przeglądowi polegającemu na ocenie ich stanu technicznego.
2. Twarde dyski sprawdza się programami narzędziowymi do wykrywania błędów i usterek. W razie braku możliwości naprawy błędu dysk podlega formatowaniu. Przy błędach pozostałych dysk czyści się zapisując z weryfikacją wszystkie sektory dysku. Jeśli błędy pozostają dysk uznaje się jako niesprawny i przeznacza do zniszczenia.
3. Płyty DVD/CD niezdatne do użytku (wykazujące błędy) przeznacza się do zniszczenia.
4. Zniszczenie nośnika określa procedura likwidacji nośników zawierających dane osobowe.

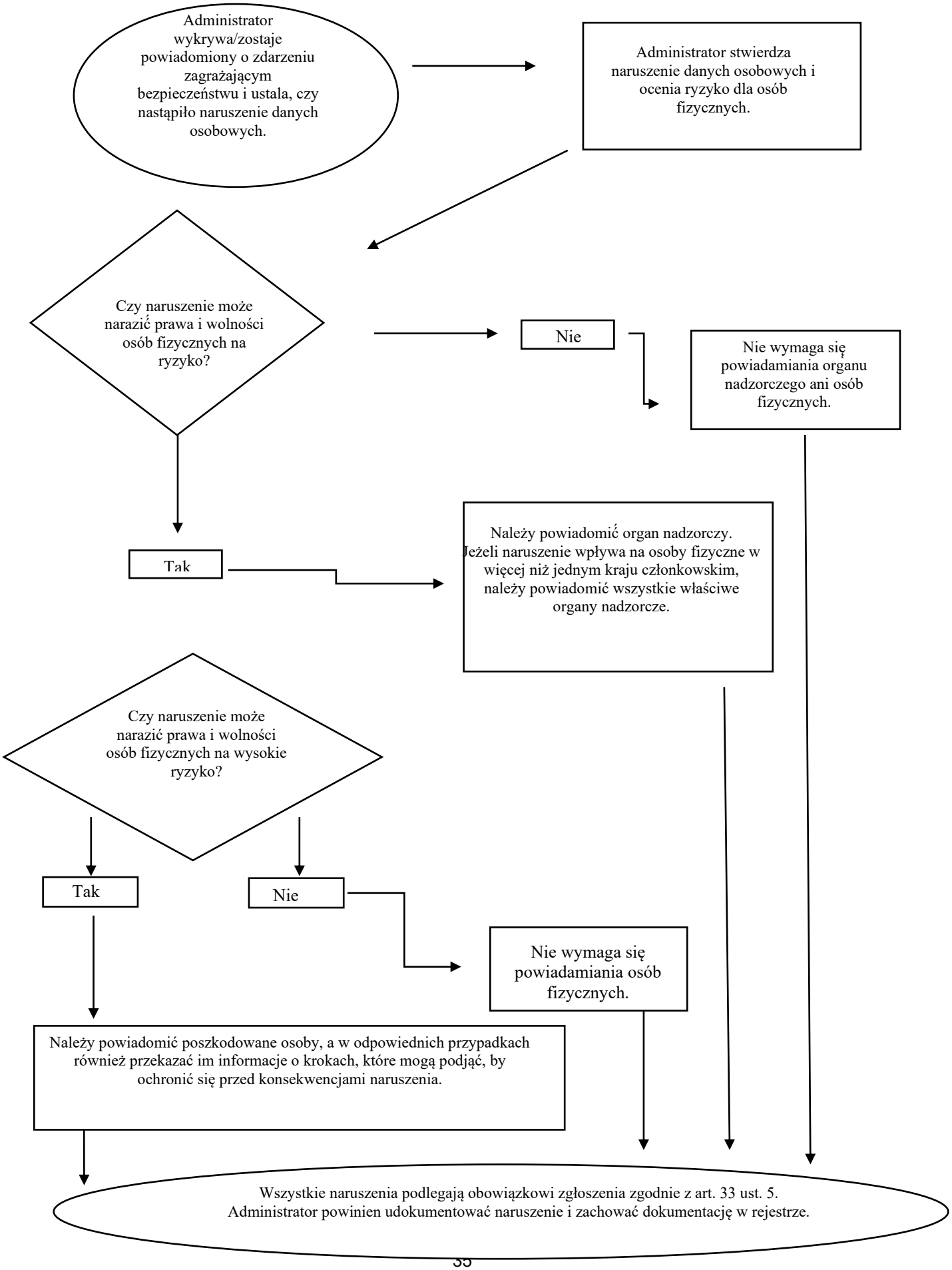
Procedura postępowania w sytuacji naruszenia ochrony danych osobowych	
numer procedury: 11	
dotyczy:	wszystkich użytkowników systemów informatycznych
osoby odpowiedzialne:	Inspektor Ochrony Danych Osobowych

1. W przypadku stwierdzenia naruszenia ochrony danych osobowych na co może wskazywać: stan urządzeń, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej należy niezwłocznie powiadomić Inspektora Ochrony Danych Osobowych.
2. Inspektor Ochrony Danych Osobowych dokonuje niezwłocznie zabezpieczenia zbiorów danych osobowych oraz logów systemów operacyjnych komputerów celem analizy.
3. Inspektora Ochrony Danych Osobowych dokona sprawdzenia czy naruszenie miało faktycznie miejsce na podstawie zebranych dowodów oraz wyjaśnień ewidencjonuje w rejestrze naruszeń i niezwłocznie powiadamia organ nadzoru nie później niż 72 godziny od momentu naruszenia i podejmuje próbę powiadomienia osoba których to naruszenie dotycz zgodnie z poniższym schematem i sporządza raportu z naruszenia ochrony danych stanowiący załącznik nr 6 i odnotowuje w rejestrze naruszeń wg poniższego wzoru.

Wzór rejestru naruszeń ochrony danych osobowych

Rejestr naruszeń ochrony danych osobowych					
Rodzaj naruszenia	Obowiązek zgłoszenia organowi nadzorczemu	Obowiązek zawiadomienia osoby, której dane dotyczą	Okoliczności naruszenia	Skutki naruszenia	Podjęte działania zaradcze
1.					
2.					
…					

4. Schemat postępowania w przypadku naruszenia ochrony danych osobowych



Procedura niszczenia zbiorów zawierających dane osobowe	
numer procedury: 12	
dotyczy:	wszystkich użytkowników
osoby odpowiedzialne:	wszystkich użytkowników

Rozporządzenia o ochronie danych osobowych nakłada na podmioty zobowiązane do jej stosowania obowiązek należytego przetwarzania takich danych, tak, aby spełniony został podstawowy cel ustawy w postaci zapewnienia każdemu ochrony dotyczących go danych osobowych. Jednym z obowiązków administratora danych osobowych w zakresie ich przetwarzania jest ich usuwanie, w momencie kiedy ustanie celowość ich przetwarzania zgodnie z wytycznymi wynikającymi z odrębnych ustaw.

Usuwanie danych osobowych, polega na:

a) trwałym, fizycznym ich zniszczeniu wraz z ich nośnikami w stopniu uniemożliwiającym ich odtworzenie przez osoby niepowołane przy zastosowaniu powszechnie dostępnych metod,
b) anonimizacji danych osobowych, zbiorów polegającej na pozbawieniu danych osobowych, ich zbiorów - cech umożliwiających identyfikację osób fizycznych, których dane dotyczą.

W zależności od nośnika, na którym przechowywane są dane osobowe, ich usuwanie polega na:

1. Dokumentacja tradycyjna (wydruki, notatki, dokumenty) - należy dokumentację zniszczyć bądź zanonimizować w sposób uniemożliwiający odczyt. Zgodnie z obowiązującą normą DIN 66399 opracowaną przez *Standards Committee for Information Technology and Applications (Komitet Normalizacyjny ds. Technik Informacyjnych i ich Zastosowań)* niszczarki stosowane do niszczenia danych osobowych powinny spełniać poniższe wymagania:

• Klasa B: Ochrona przeznaczona dla danych poufnych, przeznaczonych dla wąskiego grona odbiorców.

- Stopień 3: Nośniki z danymi chronionymi i poufnymi, a także danymi osobowymi, które wymagają większej ochrony - kategoria P-3 dla papieru,
- Stopień 4: Nośniki z danymi szczególnie chronionymi i poufnymi, a także z danymi

osobowymi, które podlegają większej ochronie, takie jak dane wrażliwe - kategoria P-4 dla papieru,

2. Nośniki optyczne (płyty CD/DVD/BLU-RAY - Analogicznie do dokumentacji tradycyjnej, należy w taki sposób zniszczyć nośnik, aby uniemożliwić odczytanie danych z płyty. W tym przypadku również zalecane jest wykorzystanie niszczarek spełniających wymagania:
   - **Klasa B**: Ochrona przeznaczona dla danych poufnych, przeznaczonych dla wąskiego grona odbiorców.
   - **Stopień 3**: Nośniki z danymi chronionymi i poufnymi, a także danymi osobowymi, które wymagają większej ochrony - kategoria O-3 dla płyt CD/DVD/BLU-RAY,
   - **Stopień 4**: Nośniki z danymi szczególnie chronionymi i poufnymi, a także z danymi osobowymi, które podlegają większej ochronie, takie jak dane wrażliwe - kategoria O-4 dla płyt CD/DVD/BLU-RAY,
3. Nośniki elektroniczne (pendrive/karty pamięci/dyski twarde SSD) - obecnie istniejące sposoby niszczenia danych można podzielić na dwie główne grupy metod:
   - Niszczenie programowe - polegające na wielokrotnym nadpisywaniu danych na nośniku, które uniemożliwiają odczytanie danych. Istnieje specjalne oprogramowanie dostępne na rynku służące do nadpisywania (definitywnego usuwania) danych.
   - Niszczenie sprzętowe - polegające na trwałym zniszczeniu nośnika za pomocą odpowiednich urządzeń.
4. Nośniki magnetyczne (dyski twarde HDD) - oprócz sposobów niszczenia danych dostępnych dla nośników elektronicznych, istnieje również możliwość demagnetyzacji nośników, jako jednego z rodzajów niszczenia sprzętowego.

5. Niezależnie od nośnika, na którym są przechowywane dane osobowe przeznaczone do zniszczenia, samo ich zniszczenie powinno odbyć się komisyjnie, a z samej operacji powinien zostać sporządzony protokół.

Procedura postępowanie w wypadku klęski żywiołowej.	
numer procedury: 13	
dotyczy:	wszystkich użytkowników przetwarzających dane osobowe

1. Klęską żywiołową jest katastrofa, spowodowana działaniem sił przyrody takich jak ogień ,huragan, woda lub ich przejawami.
2. W przypadku wystąpienia zagrożenia powodującego konieczność przeprowadzenia ewakuacji osób lub mienia z pomieszczeń , w których przetwarzane są dane osobowe, mają zastosowanie przepisy niniejszego rozdziału oraz innych przepisów szczególnych.

- zagrożeniu, jego skali i podjętych krokach zaradczych pracownik ochrony zobowiązany jest niezwłocznie powiadomić Administratora Danych Osobowych w każdy możliwy sposób. W razie niemożności skontaktowania się z nim pracownik ochrony zawiadamia, co najmniej jedną z niej wymienionych osób:

-Inspektora Ochrony Danych Osobowych

-lub inną osobę wyznaczoną przez Administratora Danych Osobowych

- Numery telefonów Administratora Danych Osobowych i Inspektora Ochrony Danych Osobowych, z którymi należy się kontaktować na wypadek klęski żywiołowej powinny być znane pracownikom.

3. Osoby biorące udział w akcji ratunkowej, mają prawo wejść do pomieszczeń w których przetwarzane są dane osobowe.
4. W przypadku ogłoszenia alarmu ewakuacyjnego użytkownicy, przebywający w pomieszczeniach, w których przetwarzane są dane osobowe, obowiązani są do przerwania pracy, a w miarę możliwości przed opuszczeniem tych pomieszczeń do:
   - Zamknięcia systemu informatycznego,
   - Zabezpieczenia danych osobowych gromadzonych w kartotekach.
5. W czasie trwania akcji ratunkowej i po jej zakończeniu Administrator Danych Osobowych czy też Inspektora Ochrony Danych Osobowych jeżeli został wyznaczony oraz obecni użytkownicy powinni, w miarę możliwości, zabezpieczać dane osobowe przed nieuprawnionym do nich dostępem.
6. Obowiązek ten ciąży w równym stopniu na innych pracownikach Administratora Danych Osobowych, obecnych przy akcji ratunkowej.

Procedura użytkowania komputerów przenośnych	
numer procedury: 14	
dotyczy:	wszystkich użytkowników przetwarzających dane osobowe

1. Pracownicy upoważnieni do przetwarzania danych osobowych i pracujący na komputerach przenośnych muszą zapoznać się z procedurą użytkowania komputera przenośnego oraz pisemnego zobowiązania się do jego przestrzegania.

2. Dane osobowe lub danych poufne muszą zostać zaszyfrowane na dysku i zabezpieczone co najmniej 8-znakowym hasłem (duże, małe litery i cyfry).

3. Komputery przenośne są wykorzystywane do prac służbowych. W przypadku konieczności korzystania z komputera przenośnego w innym celu wszystkie dane osobowe muszą być zabezpieczone hasłem.

4. W przypadku kradzieży/zgubienia lub naruszenia ochrony danych osobowych osoba upoważniona zobowiązana jest zgłosić zdarzenie/problem administratorowi bezpieczeństwa informacji.

5. Osoba upoważniona zobowiązana jest do zabezpieczenia komputera przenośnego w czasie transportu, a przede wszystkim:

1) zaleca się przenoszenie komputera przenośnego w zwykłej teczce, aktówce,

2) zabrania się pozostawiania komputera przenośnego w samochodzie podczas nieobecności osoby upoważnionej.

6. Gdy komputer przenośny jest pozostawiony w miejscu dostępnym dla osób nieupoważnionych, konieczne jest zabezpieczenie hasłem. Dotyczy to przede wszystkim zabezpieczenia komputera przenośnego na stanowisku pracy, podczas przedstawiania prezentacji, szkolenia.

7. Użytkownik komputera przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych na serwerze. Nośniki z takimi kopiami powinny być przechowywane w miejscu zabezpieczonym przed dostępem osób nieupoważnionych.

8. Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, osoba upoważniona zobowiązana jest do chronienia wyświetlanych danych osobowych na monitorze przed wglądem osób nieupoważnionych.
9. Oświadczenie o zaznajomieniu z procedurą, po podpisaniu, trafia do dokumentacji kadrowej danej osoby.

Procedura kontroli przestrzegania zasad zabezpieczenia ochrony danych osobowych	
numer procedury: 15	
dotyczy:	wszystkich użytkowników systemów informatycznych
osoby odpowiedzialne:	Inspektor Ochrony Danych Osobowych

1. Administrator Danych Osobowych zleca Inspektor Ochrony Danych Osobowych który sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych.
2. Administrator Danych Osobowych lub Inspektor Ochrony Danych Osobowych czyli osoba przez niego wyznaczona dokonuje okresowych kontroli i oceny funkcjonowania mechanizmów zabezpieczeń oraz przestrzegania zasad postępowania w przypadku naruszenia ochrony danych osobowych przynajmniej raz w roku.
3. Przedmiotem kontroli, o których mowa w ust. 2 powinno być w szczególności:
   - Funkcjonowanie zabezpieczeń systemowych,
   - Prawidłowo funkcjonowania mechanizmów kontroli dostępu do zbioru danych,
   - Funkcjonowanie zastosowanych zabezpieczeń fizycznych,
   - Zasady przechowywania kartotek,
   - Zasady i sposoby likwidacji oraz archiwizowania zbiorów archiwalnych,
   - Realizacja procedur wdrożonych przez Administratora Danych Osobowych w zakresie ochrony danych.
4. Administrator Danych Osobowych, który może zlecić to Inspektorowi Ochrony Danych Osobowych który prowadzi rejestr dokonywanych kontroli oraz ustaleń, wniosków i zaleceń z nich wynikających, a także nadzoruje ich wykonywanie.
5. Z kontroli, o których mowa w ust. 2 należy sporządzać protokoły (Załącznik nr 4 Protokół z kontroli / czynności sprawdzających w zakresie ochrony danych osobowych**)**, które przechowuje Administrator Danych Osobowych lub Inspektor Ochrony Danych Osobowych w przypadku gdy został powołany.

Załącznik 5 do polityki ochrony danych osobowych

Protokół z kontroli / czynności sprawdzających*
w zakresie ochrony danych osobowych

1. Nazwa kontrolowanej jednostki organizacyjnej:

   ……..…..

2. Zbiory danych osobowych, których przetwarzanie podlega kontroli:

   …….....

3. Data wykonania czynności kontrolnych:

   ……..…….....

4. Imię i nazwisko oraz stanowisko osoby wykonującej czynności kontrolne:

   …….....…..

5. Imiona i nazwiska osób udzielających informacji dotyczących ochrony danych osobowych w kontrolowanej komórce organizacyjnej:

   ……..……..……
   ….....…..……

6. Ustalenia dokonane w trakcie czynności kontrolnych:

   ……

   ……
   ……
   ……
   ……

7. Wnioski i zalecenia pokontrolne:

   ……
   ……
   ……
   ……
   ……

…….. (data i podpis osoby wykonującej czynności kontrolne)

…….. (data i podpis kierownika kontrolowanej kom. organizacyjnej)

Otrzymują:
1 x Kierownik kontrolowanego referatu
1 x Inspektor Ochrony Danych Osobowych

* niepotrzebne skreślić

Załącznik 6 do polityki ochrony danych osobowych

Wzór raportu z naruszenia ochrony danych

1. Data ……. Godzina ……

2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem (imię, nazwisko, stanowisko służbowe):

……..

3. Lokalizacja zdarzenia (nr pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):

……

4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:

……

5. Podjęte działania:

……

6. Wstępna ocena przyczyn wystąpienia naruszenia:

…….

7. Postępowanie wyjaśniające i naprawcze:

…….

……. …….

(podpis pracownika) *(data i podpis inspektora ochrony danych)*

Załącznik 7 do polityki ochrony danych osobowych

Wzór rejestru realizacji żądań podmiotu danych

I. Żądanie

1. Data zgłoszenia żądania:

……...

2. Forma zgłoszenia żądania (kanał komunikacji):

……...

3. Zgłaszający żądanie:

……...

4. Treść żądania:

……...

II. Obsługa żądania

1. Pracownik obsługujący żądanie:

……...

2. Czy dane zgłaszającego żądanie są przetwarzane przez administratora danych:

……...

3. Czy dane zgłaszającego żądanie zostały powierzone (komu, kiedy):

……...

4. Podjęte czynności:

a) Czynność I

- Osoba podejmująca czynność:

……...

- Opis czynności:

……...

- Data dokonania czynności:

……...

b) Czynność II

- Osoba podejmująca czynność:

……...

- Opis czynności:

……...

- Data dokonania czynności:

……

Załącznik 8 do polityki ochrony danych osobowych

Zgoda na podpowierzenie

[*Nazwa administratora danych*] wyraża zgodę na skorzystanie przez [*nazwa podmiotu przetwarzającego*] z usług innego podmiotu przetwarzającego o nazwie [*nazwa podmiotu podprzetwarzającego*] w zakresie przetwarzania danych osobowych powierzonych [*nazwa podmiotu przetwarzającego*].

Wzór ogólnej klauzuli zgody na podpowierzenie

1. *[Nazwa administratora danych*] wyraża zgodę na korzystanie przez [*nazwa podmiotu przetwarzającego*] z usług innych podmiotów przetwarzających w zakresie przetwarzania danych osobowych powierzonych [*nazwa podmiotu przetwarzającego*].
2. [*Nazwa podmiotu przetwarzającego*] zobowiązany jest do informowania [*nazwa administratora danych*] o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających.
3. [*Nazwa podmiotu przetwarzającego*] ma prawo dokonać zmiany dotyczącej dodania lub zastąpienia innego podmiotu przetwarzającego, jeśli [*nazwa administratora danych*] nie wyrazi sprzeciwu wobec zmiany w terminie dwóch tygodni od dnia otrzymania informacji o zamierzonej zmianie, o której mowa w pkt 2 powyżej.
4. Wzór sprzeciwu, o którym mówi pkt 3 powyżej stanowi Załącznik [X] do niniejszej umowy.

Załącznik 9 do polityki ochrony danych osobowych

Wzór klauzuli informacyjnej stosowanej po rozpoczęciu stosowania RODO – w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą

Informuję, że:

1) administratorem Pani/Pana danych osobowych jest …… z siedzibą w …… przy ul. ……, zwany dalej Administratorem; Administrator prowadzi operacje przetwarzania następujących kategorii Pani/Pana danych osobowych:
    - …,
    - …,
2) inspektorem danych osobowych u Administratora jest ……, e-mail: ……,
3) Pani/Pana dane osobowe przetwarzane będą w celu …… i nie będą udostępniane innym odbiorcom,
4) podstawą przetwarzania Pani/Pana danych osobowych jest ……,
5) Administrator pozyskał Pani/Pana dane osobowe od …… z siedzibą w …… przy ul. ……,
6) posiada Pani/Pan prawo do:
    - żądania od Administratora dostępu do swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych,
    - wniesienia sprzeciwu wobec takiego przetwarzania,
    - przenoszenia danych,
    - wniesienia skargi do organu nadzorczego,
    - cofnięcia zgody na przetwarzanie danych osobowych.
7) Pani/Pana dane osobowe nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu,
8) Pani/Pana dane osobowe będą przechowywane przez ……

Załącznik 10 do polityki ochrony danych osobowych

Wzór klauzuli informacyjnej stosowanej po rozpoczęciu stosowania RODO – w przypadku zbierania danych od osoby, której dane dotyczą

Informuję, że:

1) administratorem Pani/Pana danych osobowych jest …… z siedzibą w …… przy ul. ……, zwany dalej Administratorem; Administrator prowadzi operacje przetwarzania Pani/Pana danych osobowych,
2) inspektorem danych osobowych u Administratora jest ……, e-mail: ……,
3) Pani/Pana dane osobowe przetwarzane będą w celu …… i nie będą udostępniane innym odbiorcom,
4) podstawą przetwarzania Pani/Pana danych osobowych jest ……,
5) podanie danych jest niezbędne do zawarcia umowy, w przypadku niepodania danych niemożliwe jest zawarcie umowy,
6) posiada Pani/Pan prawo do:

- żądania od Administratora dostępu do swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych,
- wniesienia sprzeciwu wobec takiego przetwarzania,
- przenoszenia danych,
- wniesienia skargi do organu nadzorczego,
- cofnięcia zgody na przetwarzanie danych osobowych.

7) Pani/Pana dane osobowe nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu,
8) Pani/Pana dane osobowe będą przechowywane przez ……

Załącznik 11 do polityki ochrony danych osobowych

Wzór klauzuli zgody na przetwarzanie danych osobowych zgodnej z RODO

1. Wyrażam zgodę na przetwarzanie moich danych osobowych przez administratora danych …… z siedzibą w ……, ul. ……, numer KRS ……. w celu ……
2. Podaję dane osobowe dobrowolnie i oświadczam, że są one zgodne z prawdą.
3. Zapoznałem(-am) się z treścią klauzuli informacyjnej, w tym z informacją o celu i sposobach przetwarzania danych osobowych oraz prawie dostępu do treści swoich danych i prawie ich poprawiania.

Załącznik 12 do polityki ochrony danych osobowych

Klauzula odpowiedzialności w umowie podpowierzenia

Po zawarciu umowy podpowierzenia danych Przetwarzający będzie ponosił odpowiedzialność za działania i zaniechania osoby trzeciej, której podpowierzył dane, jak za własne działania i zaniechania. Odpowiedzialność Przetwarzającego i osoby trzeciej, której podpowierzono dane, jest odpowiedzialnością solidarną.

Załącznik 13 do polityki ochrony danych osobowych

Klauzula dotycząca kontroli wykonywania umowy przez procesora

1. Administrator jest uprawniony do kontrolowania sposobu wykonania umowy o powierzenie danych osobowych przez procesora oraz przestrzegania obowiązujących przepisów prawa z zakresu ochrony danych osobowych.
2. W celu wykonania kontroli upoważnieni pracownicy administratora mają prawo:
1) wstępu do pomieszczeń, w których procesor przetwarza powierzone dane osobowe, żądania złożenia pisemnych i ustnych wyjaśnień w celu ustalenia stanu faktycznego,
2) przeprowadzenia oględzin dokumentów, a także urządzeń, nośników oraz systemów informatycznych służących do przetwarzania powierzonych danych.

Załącznik 14 do polityki ochrony danych osobowych

Wzór rejestru wszystkich kategorii czynności przetwarzania danych dokonywanych w imieniu administratora

Rejestr wszystkich kategorii czynności przetwarzania danych dokonywanych w imieniu administratora	
Imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego	
Imię i nazwisko lub nazwa oraz dane kontaktowe każdego administratora, w którego imieniu działa podmiot przetwarzający	
Imię i nazwisko lub nazwa oraz dane kontaktowe przedstawiciela podmiotu przetwarzającego lub administratora	
Imię i nazwisko oraz dane kontaktowe inspektora ochrony danych	
Kategorie przetwarzań dokonywanych w imieniu każdego z administratorów	
Przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa lub organizacji międzynarodowej	
Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa	

Załącznik 15 do polityki ochrony danych osobowych

Wykaz podmiotów zewnętrznych, którym powierzono dane do przetwarzania

Wykaz firm/zleceniobiorców/wykonawców, z którymi realizacja umów/porozumień/zamówień zobowiązuje lub umożliwia dostęp do informacji zawierających dane osobowe

Lp.	**Nazwa firmy**	**Zakres świadczonych usług**	**Numer/data umowy**	**Uwagi** (czy są zapisy w umowie związane z poufnością i odpowiedzialnością w stosunku do powierzonych danych, czy jest umowa powierzenia)
1.				
2.				
…				