Załącznik Nr 1
do Zarządzenia Nr 5/XII2021
Dyrektora Gminnego Centrum
Kultury i Sportu w Ostrowie
z/s w Kamionce
z dnia 1 grudnia 2021 roku

POLITYKA BEZPIECZEŃSTWA
PRZETWARZANIA DANYCH OSOBOWYCH
W
GMINNYM CENTRUM KULTURY I SPORTU W OSTROWIE
Z/S W KAMIONCE

2021

SPIS TREŚCI

ROZDZIAŁ I
POSTANOWIENIA OGÓLNE

§ 1.

„Polityka bezpieczeństwa przetwarzania danych osobowych w Gminnym Centrum Kultury i Sportu w Ostrowie z/s w Kamionce" zwana dalej „Polityką", zawiera zasady przetwarzania danych osobowych oraz zabezpieczenia techniczne i organizacyjne zarówno zabezpieczenia danych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemach informatycznych, które mają zapewnić poufność, integralność, dostępność, rozliczalność, autentyczność, niezaprzeczalność, niezawodność ochrony danych osobowych w Gminnym Centrum Kultury i Sportu w Ostrowie z/s w Kamionce, zwanym dalej „GCKiS".

§ 2.

1. Definicje w „Polityce "oznaczają:

   1) **Administrator Danych Osobowych** (zwany dalej **ADO** lub **Administrator**) – GCKiS, reprezentowany przez Dyrektora;

   2) **Inspektor Danych Osobowych** (zwany dalej **IOD**) – osoba, której ADO powierzył wykonywanie funkcji IOD, o której mowa w rozdziale IV sekcja 4 RODO;

   3) **Administrator Systemu Informatycznego** (zwany dalej **ASI**) – osoba odpowiedzialna za nadzór nad zabezpieczeniem przetwarzania danych osobowych w systemie informatycznym Administratora;

   4) **autentyczność** – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów i informacji);

   5) **bezpieczeństwo przetwarzania danych osobowych** – zachowanie poufności, integralności i rozliczalności danych osobowych, mogą być również brane pod uwagę inne właściwości, takie jak dostępność, autentyczność, niezaprzeczalność i niezawodność;

   6) **dane osobowe** – oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

   7) **PUODO** – Prezes Urzędu Ochrony Danych Osobowych;

   8) **integralność danych** – właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

9) **dostępność** – zapewnienie bycia osiągalnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot;

10) **naruszenie ochrony danych osobowych** – zamierzone lub przypadkowe naruszenie środków technicznych i organizacyjnych zastosowanych w celu ochrony danych osobowych w szczególności, gdy stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszanie ochrony danych osobowych;

11) **niezaprzeczalność** – brak możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych osobowych przez jeden z podmiotów uczestniczących w tej wymianie;

12) **niezawodność** – zapewnienie spójności oraz zamierzonych zachowań i skutków;

13) **poufność** – właściwość zapewniająca, że informacja (np. dane osobowe) jest dostępna tylko podmiotom upoważnionym;

14) **przetwarzanie danych osobowych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, przede wszystkim te, które wykonuje się w systemach informatycznych;

15) **rozliczalność** – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

16) **system informatyczny administratora danych (**zwany dalej **systemem informatycznym) –** sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer lub komputer centralny, system ten tworzy sieć teleinformatyczną administratora danych;

17) **system tradycyjny** – dokumentacja w wersji papierowej, w szczególności w formie kartoteki, skorowidza, księgi, wykazu lub innego zbioru ewidencyjnego;

18) **ustawa** – ustawa z 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781);

19) **użytkownik systemu** – osoba upoważniona do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym, która posiada ustalony identyfikator i hasło;

20) **użytkownik zewnętrzny** – osoba nie będącą pracownikiem posiadającą uprawnienia do przetwarzania danych;

21) **zbiór danych osobowych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny wg określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie;

22) **dokumenty powiązane** – odrębne dokumenty dotyczące bezpieczeństwa ochrony danych powiązane z „Polityką" np. „Instrukcja zarządzania systemem informatycznym", „Polityka czystego biurka i druku";

23) **serwisant** – firma lub pracownik firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu informatycznego oraz oprogramowania;

24) **ISO/IEC 27001**[1] – norma międzynarodowa standaryzująca systemy zarządzania bezpieczeństwem informacji;

25) **RODO** – 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).

26) **RCPD** – Rejestr Czynności Przetwarzania Danych.

2. Celem *Polityki* jest zapewnienie należytej ochrony danych osobowych zgromadzonych w zasobach ADO, wskazanie działań, jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie zabezpieczyć dane osobowe[2].

3. *Polityka* zawiera:
   1) oświadczenie o intencjach ADO potwierdzające cele i zasady bezpieczeństwa informacji w odniesieniu do strategii i wymagań;
   2) strukturę wyznaczania celów stosowania zabezpieczeń, w tym strukturę szacowania i zarządzania ryzykiem;
   3) zasady, normy i wymagania zgodności mających szczególne znaczenie dla ADO zawierające:
      a) zgodność z prawem, regulacjami wewnętrznymi i wymaganiami wynikającymi z umów;
      b) wymagania dotyczące kształcenia, szkoleń i uświadamiania w dziedzinie bezpieczeństwa;
      c) zarządzanie ciągłością działania ADO;
      d) konsekwencje naruszenia „*Polityki bezpieczeństwa*" oraz dokumentów powiązanych;
   5) definicje ogólnych i szczególnych obowiązków w odniesieniu do zarządzania bezpieczeństwem informacji, w tym zgłaszania incydentów związanych z bezpieczeństwem danych;
   6) obowiązek przestrzegania przez użytkowników zasad bezpieczeństwa.

[1] W niniejszej Normie Międzynarodowej podano zalecenia dotyczące standardów bezpieczeństwa informacji w organizacjach i praktyk zarządzania bezpieczeństwem informacji, w tym wyboru, wdrażania i zarządzania zabezpieczeniami, z uwzględnieniem środowiska (środowisk), w którym (których) w organizacji występuje (-ą) ryzyko w bezpieczeństwie informacji. Niniejsza Norma Międzynarodowa jest przeznaczona do stosowania przez organizacje, które zamierzają:
a) wybierać zabezpieczenia w ramach procesu wdrażania Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z ISO/IEC 27001 [10];
b) wdrażać powszechnie akceptowane zabezpieczenia informacji;
c) opracować własne zalecenia w zakresie zarządzania bezpieczeństwem informacji.

[2] art. 32 RODO.

4. Zasady określone w *Polityce* oraz w dokumentach powiązanych powinny być znane i stosowane przez pracowników bez względu na zajmowane stanowisko, miejsce wykonywanej pracy, charakter stosunku pracy oraz w niezbędnym zakresie przez współpracowników przetwarzających dane osobowe.
5. Odpowiedzialnym za wdrożenie i utrzymanie niniejszej Polityki jest ADO, w tym za bieżącą, operacyjną ochronę danych osobowych odpowiada, każda osoba przetwarzająca dane w zakresie zgodnym z zakresem upoważnienia, kompetencjami lub rolą sprawowaną w procesie przetwarzania danych.

§ 3.

1. *Polityka* oraz dokumenty z nią powiązane powinny być aktualizowane na bieżąco wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych.
2. Przegląd *Polityki* ma na celu stwierdzenie, czy zawarte w niej postanowienia odpowiadają aktualnej i planowanej działalności ADO.
3. Fakty wystąpienia poważnych naruszeń ochrony danych osobowych powinny skutkować zmianami w *Polityce* i dokumentach powiązanych.

§ 4.

Na każdym etapie przetwarzania danych osobowych należy brać pod uwagę w niezbędnym zakresie, integralność, poufność oraz rozliczalność dla przetwarzanych danych osobowych.

ROZDZIAŁ II

PRZETWARZANIE DANYCH OSOBOWYCH

A. ZASADY PRZETWARZANIA DANYCH[3]

§ 5.

1. W zakresie zasad dotyczących przetwarzania danych osobowych do obowiązków ADO należy, aby dane osobowe były:
   1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);
   2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dozwolone jest dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych, historycznych lub do celów statystycznych;

[3] art. 5 RODO.

3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);
4) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);
5) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy o ile będą one przetwarzane wyłącznie do celów archiwalnych;
6) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”).

2. Administrator jest odpowiedzialny za przestrzeganie zasad, wynikających z ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność”).

B. ZGODNOŚĆ PRZETWARZANIA Z PRAWEM[4]

§ 6.

1. Przetwarzanie danych osobowych przez ADO jest zgodne z prawem wyłącznie w przypadkach, gdy spełniony jest co najmniej jeden z poniższych warunków:
   1) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów[5];
   2) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą przed zawarciem umowy;
   3) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na ADO;
   4) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
   5) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej ADO;
   6) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez ADO lub przez stronę trzecią z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

[4] art. 6 RODO.
[5] Wzór - Załącznik **Nr 1** do Polityki „*Oświadczenie osoby wyrażającej zgodę na przetwarzanie jej danych osobowych*”.

2. Jeżeli przetwarzanie w celu innym niż cel, w którym dane osobowe zostały zebrane, nie odbywa się na podstawie zgody osoby, której dane dotyczą, ani prawa Unii Europejskiej lub prawa państwa członkowskiego stanowiących w demokratycznym społeczeństwie niezbędny i proporcjonalny środek służący zagwarantowaniu celów, ADO – aby ustalić, czy przetwarzanie w innym celu jest zgodne z celem, w którym dane osobowe zostały pierwotnie zebrane – bierze pod uwagę między innymi:
   1) wszelkie związki między celami, w których zebrano dane osobowe, a celami zamierzonego dalszego przetwarzania;
   2) kontekst, w którym zebrano dane osobowe, w szczególności relację między osobami, których dane dotyczą, a ADO;
   3) charakter danych osobowych, w szczególności czy przetwarzane są szczególne kategorie danych osobowych;
   4) ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą;
   5) istnienie odpowiednich zabezpieczeń, w tym ewentualnie szyfrowania lub pseudonimizacji.
3. ADO identyfikuje przypadki, w których przetwarza lub może przetwarzać szczególne kategorie danych osobowych oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania danych wrażliwych. W sytuacji zidentyfikowania przypadków przetwarzania danych wrażliwych, ADO postępuje zgodnie z przyjętymi zasadami w tym zakresie, respektując w szczególności zapisy art. 9 i art. 10 RODO.

ROZDZIAŁ III
PRAWA OSÓB, KTÓRYCH DOTYCZĄ

A. OBOWIĄZEK INFORMACYJNY[6]

§ 7.

1. ADO zobowiązany jest stosować przejrzyste informowanie, komunikację oraz tryb wykonywania praw przez osobę, której dane osobowe są przetwarzane.
2. ADO podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności gdy informacje są kierowane do dziecka – udzielić osobie[7], której dane dotyczą, wszelkich informacji oraz powiadomić osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych nie od tej osoby[8].
3. Informacji udziela się na piśmie. W miarę możliwości informacje także są przekazywane elektronicznie, w uzasadnionych przypadkach informacja może zostać przekazana ustnie.

[6] Art. 13-14 RODO.
[7] Wzór - Załącznik Nr 2 do Polityki *„Informacja o zbieraniu danych osobowych od osoby, której dane dotyczą”.*
[8] Wzór - Załącznik Nr 3 do Polityki „*Informacja o zbieraniu danych osobowych nie od osoby, której dane dotyczą*”.

4. ADO bez zbędnej zwłoki – w terminie miesiąca od otrzymania żądania – udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem[9]:
   1) w razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań;
   2) w terminie miesiąca od otrzymania żądania ADO informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie chyba, że osoba, której dane dotyczą zażąda innej formy.

§ 8.

1. Jeżeli dane osobowe osoby, której dane dotyczą pozyskane są od tej osoby, ADO podaje osobie następujące informacje:
   1) swoją tożsamość i dane kontaktowe;
   2) dane kontaktowe IOD;
   3) cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania;
   4) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) RODO – prawnie uzasadnione interesy realizowane przez ADO lub przez stronę trzecią;
   5) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców;
   6) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz informację o sposobach uzyskania kopii tych zabezpieczeń lub o miejscu ich udostępnienia;
   7) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
   8) informacje o prawie do żądania od ADO dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia, ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
   9) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
   10) informacje o prawie wniesienia skargi do organu nadzorczego;

[9] Wzór - Załącznik Nr 4 do Polityki „*Informacja o przetwarzaniu danych osobowych osoby”.*

11) informację, czy podanie danych osobowych jest wymogiem ustawowym, umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
12) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu.

2. Nie ma zastosowania ust. 1 gdy – i w zakresie, w jakim – osoba, której dane dotyczą, dysponuje już tymi informacjami.

3. Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, ADO podaje osobie, której dane dotyczą następujące informacje:
   1) swoją tożsamość i dane kontaktowe;
   2) dane kontaktowe IOD;
   3) cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania;
   4) kategorie odnośnych danych osobowych;
   5) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f RODO – prawnie uzasadnione interesy realizowane przez ADO lub przez stronę trzecią;
   6) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców;
   7) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz informację o sposobach uzyskania kopii tych zabezpieczeń lub o miejscu ich udostępnienia;
   8) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
   9) informacje o prawie do żądania od ADO dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia, ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
   10) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a RODO lub art. 9 ust. 2 lit. a RODO – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
   11) informacje o prawie wniesienia skargi do organu nadzorczego;
   12) źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych;
   13) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu.

4. Nie ma zastosowania ust. 3, gdy – i w zakresie, w jakim:
   1) osoba, której dane dotyczą, dysponuje już tymi informacjami;
   2) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku;

3) pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii Europejskiej lub prawem państwa członkowskiego, któremu podlega Administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą;
4) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii Europejskiej lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.

5. Jeżeli ADO planuje dalej przetwarzać dane osobowe, w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje ona osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji.
6. Nie ma zastosowania ust. 5 gdy wystąpią przesłanki przewidziane w ust. 4.

B. PRAWO DOSTĘPU PRZYSŁUGUJĄCE OSOBIE, KTÓREJ DANE DOTYCZĄ[10]

§ 9.

1. Osoba, której dane dotyczą jest uprawniona do uzyskania od ADO potwierdzenia, czy przetwarzane są jej dane osobowe, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do tych danych oraz następujących informacji dotyczących[11]:
   1) celu przetwarzania;
   2) kategorii odnośnych danych osobowych;
   3) informacji o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
   4) w miarę możliwości planowanych okresów przechowywania danych osobowych, a gdy nie jest to możliwe, kryteriów ustalania tego okresu;
   5) informacji o prawie do żądania od ADO sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
   6) informacji o prawie wniesienia skargi do organu nadzorczego;
   7) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkich dostępnych informacji o ich źródle;
   8) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu.
2. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach.
3. ADO dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu:

[10] art. 15 RODO.
[11] Wzór - Załącznik **Nr 4** do Polityki „*Informacja o przetwarzaniu danych osobowych”.*

1) za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą ADO może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych;
2) jeżeli osoba, której dane dotyczą zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się drogą elektroniczną.

C. PRAWO DO SPROSTOWANIA DANYCH[12]

§ 10.

1. Osoba, której dane dotyczą, ma prawo żądania od ADO niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe.
2. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

D. PRAWO DO USUNIĘCIA DANYCH[13] („prawo do bycia zapomnianym")

§ 11.

1. Osoba, której dane dotyczą, ma prawo żądania od ADO niezwłocznego usunięcia dotyczących jej danych osobowych, natomiast ADO ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:
   1) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
   2) osoba, której dane dotyczą cofnęła zgodę, na której opiera się przetwarzanie[14] i nie ma innej podstawy prawnej przetwarzania;
   3) osoba, której dane dotyczą wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania;
   4) dane osobowe były przetwarzane niezgodnie z prawem;
   5) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii Europejskiej lub prawie państwa członkowskiego, któremu podlega Administrator;
2. Jeżeli ADO upublicznił dane osobowe, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować Administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by Administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

[12] art. 16 RODO.
[13] art. 17 RODO.
[14] art. 6 ust. 1 lit. a), lub art. 9 ust. 2 lit. a) RODO.

E. PRAWO DO OGRANICZENIA PRZETWARZANIA[15]

§ 12.

1. Osoba, której dane dotyczą, ma prawo żądania od ADO ograniczenia przetwarzania w następujących przypadkach:
   1) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający ADO 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) ADO 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 wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie ADO są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.
2. Jeżeli przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą lub w celu ustalenia, dochodzenia lub obrony roszczeń, albo w celu ochrony praw innej osoby fizycznej lub prawnej, a także z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.
3. Przed uchyleniem ograniczenia przetwarzania ADO informuje o tym osobę, której dane dotyczą, która żądała ograniczenia.

F. OBOWIĄZEK POWIADOMIENIA O SPROSTOWANIU LUB USUNIĘCIU DANYCH OSOBOWYCH LUB O OGRANICZENIU PRZETWARZANIA[16]

§ 13.

1. ADO informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.
2. ADO informuje osobę, której dane dotyczą o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

[15] art. 18 RODO.
[16] art. 19 RODO.

G. PRAWO DO PRZENOSZENIA DANYCH[17]

§ 14.

1. Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła ADO, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony ADO, który dostarczył te dane osobowe, jeżeli:
   1) przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy[18];
   2) przetwarzanie odbywa się w sposób zautomatyzowany.
2. Wykonując prawo do przenoszenia danych, osoba, której dane dotyczą, ma prawo żądania by dane osobowe zostały przesłane przez ADO bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.

H. PRAWO DO SPRZECIWU[19]

§ 15.

1. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f) RODO.
2. W przypadku wniesienia sprzeciwu ADO nie wolno już przetwarzać tych danych osobowych chyba, że wykaże istnienie ważnych, prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia albo obrony roszczeń.
3. 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 osobowych na potrzeby takiego marketingu, w zakresie w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.
4. Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów.

[17] art. 20 RODO
[18] art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a lub art. 6 ust. 1 lit. b RODO.
[19] art. 21 RODO.

5. Najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie, o którym mowa w ust. 1 i 2 oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji.
6. W związku z korzystaniem z usług społeczeństwa informacyjnego osoba, której dane dotyczą, może wykonać prawo do sprzeciwu za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne.

ROZDZIAŁ IV
UDOSTĘPNIANIE DANYCH OSOBOWYCH

§ 16.

1. Dane osobowe mogą być udostępnione podmiotom uprawnionym na mocy obowiązujących przepisów prawa do ich otrzymania, jeżeli w sposób wiarygodny, uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których te dane dotyczą.
2. Dane osobowe udostępnia się na podstawie pisemnego bądź elektronicznego wniosku, chyba że przepisy prawa stanową inaczej.
3. Każda czynność związana z udostępnieniem danych podlega zarejestrowaniu.
4. Odpowiedzialnym za udzielenie odpowiedzi na wniosek, o którym mowa w ust. 2, jest pracownik, któremu przypisano daną sprawę.
5. Dopuszczona jest forma udostępniania danych osobowych w trybie on-line za pomocą usług sieciowych lub wymiany plików, pod warunkiem zachowania standardów gwarantujących bezpieczeństwo przekazywanych danych, zgodnie z procedurą udostępniania danych.
6. Udostępnianie danych osobowych w trybie on-line możliwe jest dopiero po wcześniejszym uzgodnieniu i potwierdzeniu w formie pisemnej zasad udostępniania danych osobowych z uwzględnieniem takich przesłanek jak zapewnienie legalności, poufności i integralności udostępnianych danych, pod warunkiem możliwości ustalenia w każdym czasie, jakie dane zostały przekazane i kto tego dokonał.
7. Wszelkie udostępnianie instytucjom danych osobowych powinno odbywać się przy zachowaniu szczególnych środków ostrożności, które uniemożliwiają osobom nieupoważnionym wgląd do ww. danych.
8. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach związanych z przekazaniem.
9. Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić, gdy Komisja Europejska stwierdzi, że to państwo trzecie, terytorium lub określony sektor lub określone

sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony.

10. Po identyfikacji wszystkich podmiotów przetwarzających należy zweryfikować, w których przypadkach ma miejsce powierzenie przetwarzania danych osobowych do podmiotów międzynarodowych oraz czy w związku z tym są one przetwarzane w państwie trzecim. W takim przypadku niezbędna jest weryfikacja czy Komisja Europejska wydała decyzję na temat danego państwa.

ROZDZIAŁ V

ADMINISTRATOR, WSPÓŁADMINISTRATOR ORAZ PODMIOT PRZETWARZAJĄCY

A. OBOWIĄZKI ADMINISTRATORA[20]

§ 17.

Administrator ma obowiązek:

1) zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Administratora;
2) przeprowadzać i dokumentować analizę adekwatności środków bezpieczeństwa danych osobowych, w tym celu ADO powinien:
   a) zapewnić odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania − wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych;
   b) kategoryzować dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają;
   c) przeprowadzać analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii;
3) analizować 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;
4) ustalać możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa, ocenić koszty ich wdrażania oraz ustalić przydatność i stosowanie takich środków i podejścia jak:
   a) pseudonimizacja;
   b) szyfrowanie danych osobowych;
   c) inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności, odporności systemów i usług przetwarzania;
   d) 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;

[20] art. 24 RODO.

5) dokonać oceny skutków[21] planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka[22] prawdopodobieństwo naruszenia praw i wolności osób jest wysokie;
6) stosowania metodyki oceny skutków przyjętych przez ADO;
7) stosować procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych Osobowych w terminie 72 godzin od ustalenia naruszenia.

§ 18.

1. Administrator deklaruje zaangażowanie w prawidłowym zarządzaniu bezpieczeństwem informacji zgodnie z Polską Norma 27001:2014-12 – System Zarządzania Bezpieczeństwem Informacji (SZBI), która spełnia wymagania określone w § 20 Rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[23].
2. Szczegółowy zakres uprawnień, obowiązków i procedur postępowania ADO:
   1) System Zarządzania Bezpieczeństwem Informacji – w zastosowaniu praktyki codziennej:
      a) instruktaże wstępne dla nowozatrudnionych, szkolenia okresowe[24];
      b) okresowe sprawdziany wiedzy pracowników[25];
      c) monitorowanie przestrzegania zasad przez pracowników[26];
      d) analiza raportów z systemów bezpieczeństwa IT;
      e) monitoring umów z dostawcami produktów i usług;
      f) monitoring zarządzania podatnościami technicznymi;
      g) analiza incydentów;
      h) audyty SZBI;
      i) przeglądy zarządzania.
   2) Krajowe Ramy Interoperacyjności przez zapewnienie warunków umożliwiających realizację i egzekwowanie następujących działań:
      a) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
      b) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmują ich rodzaj i konfigurację[27];

[21] Wzór - Załącznik **Nr 5** do Polityki „*Ocena skutków naruszenia*".
[22] Wzór - Załącznik **Nr 6** do Polityki „*Ocena ryzyka naruszenia*".
[23] tj. Dz. U. 2017 r. poz. 2247.
[24] Wzór - Załącznik **Nr 7** do Polityki „*Lista osób uczestniczących w szkoleniu z zakresu ochrony danych osobowych*".
[25] Wzór - Załącznik **Nr 8** do Polityki „*Ankieta sprawdzenia wiedzy pracownika z zakresu ochrony danych osobowych*".
[26] Wzór - Załącznik **Nr 9** do Polityki „*Raport ze sprawdzenia zgodności z przepisami ochrony danych*."

c) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;

d) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji[28];

e) bezzwłocznej zmiany uprawnień w przypadku zmiany zadań osób, o których mowa w lit. d;

f) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:

- zagrożenia bezpieczeństwa informacji;
- skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna;
- stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

3) zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, poprzez:

a) monitorowanie dostępu do informacji;

b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji;

c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji.

4) ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;

5) zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;

6) zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji[29];

7) ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;

8) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:

---

[27] Wzór - Załącznik **Nr 10** do Polityki ”*Inwentaryzacja zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych*”.

[28] Załącznik Nr 2 do Zarządzenia Nr ..... Dyrektora Gminnego Centrum Kultury i Sportu w Ostrowie z/s w Kamionce z dn. ..... r. - „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Gminnym Centrum Kultury i Sportu w Ostrowie z/s w Kamionce” *(„Upoważnienie Nr ..... /..... do przetwarzania danych osobowych”).*

[29] Wzór - Załącznik **Nr 11** do Polityki „*Rejestr umów powierzenia przetwarzania danych*”;
Wzór - Załącznik **Nr 11a** do Polityki „*Umowa powierzenia przetwarzania danych”;*
Wzór - Załącznik **Nr 11b** do Polityki „U*mowa o współadministrowanie danymi osobowymi”.*

a) dbałości o aktualizację oprogramowania;
b) minimalizowaniu ryzyka utraty informacji w wyniku awarii;
c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją;
d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa;
e) zapewnieniu bezpieczeństwa plików systemowych;
f) redukcji ryzyka wynikającego z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych;
g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa;
h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i „Polityką bezpieczeństwa".

9) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i ustalony sposób, umożliwiający szybkie podjęcie działań korygujących[30];
10) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok,
11) stosowania podstawowych zasad jako filarów ochrony danych osobowych w zakresie:
a) legalności – ochrony prywatności i przetwarzania danych zgodnie z prawem;
b) bezpieczeństwa – zapewnienia odpowiedniego poziomu bezpieczeństwa danych podejmując stale działania w tym zakresie;
c) prawa jednostki − umożliwienia osobom, których dane przetwarza, wykonywanie swoich praw i realizacja tych praw;
d) rozliczalności − dokumentowanie, w jaki sposób administrator spełnia obowiązki, aby w każdej chwili móc wykazać zgodność;
e) rzetelności – rzetelne i uczciwe przetwarzanie danych;
f) transparentności – informowanie w sposób przejrzysty dla osoby, której dane dotyczą;
g) minimalizacji – przetwarzania w konkretnych celach i nie „na zapas";
h) adekwatności – przetwarzania danych nie więcej niż potrzeba;
i) prawidłowości – przetwarzania z dbałością o prawidłowość danych;
j) czasu – przechowywania nie dłużej niż potrzeba.

3. System zarządzania bezpieczeństwem informacji powinien być opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001[31].

[30] Załącznik Nr 3 do Zarządzenia Nr ..... Dyrektora Gminnego Centrum Kultury i Sportu w Ostrowie z/s w Kamionce z dn. ..... r. - „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Gminnym Centrum Kultury i Sportu w Ostrowie z/s w Kamionce" (*„Rejestr incydentów bezpieczeństwa oraz działań korygujących i zapobiegawczych*").
[31] § 20 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. *w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*.

4. Jeżeli system informatyczny połączony jest z siecią publiczną[32] należy stosować wysoki poziom bezpieczeństwa przetwarzania danych osobowych.

B. WSPÓŁADMINISTRATORZY[33]

§ 19.

1. Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami.
2. W drodze wspólnych uzgodnień współadministratorzy powinni w przejrzysty sposób określić odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z ochrony danych osobowych, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji[34], chyba że przypadające im obowiązki i ich zakres określa prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą.
3. Uzgodnienia, o których mowa w ust. 1, powinny odzwierciedlać odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi, a podmiotami, których dane dotyczą. Zasadnicza treść uzgodnień powinna być udostępniana podmiotom, których dane dotyczą[35].

C. PODMIOT Przetwarzający[36]

§ 20.

1. W przypadku, gdy przetwarzanie ma być dokonywane w imieniu ADO, wtedy korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.
2. Podmiot przetwarzający nie może korzystać z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody ADO. W przypadku ogólnej pisemnej zgody podmiot przetwarzający ma obowiązek poinformować ADO o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym ADO możliwość wyrażenia sprzeciwu wobec takich zmian.

---

[32] art. 25 RODO.
[33] art. 26 RODO.
[34] art. 13 i 14 RODO.
[35] Wzór - Załącznik **Nr 11b** do Polityki „U*mowa o współadministrowanie danymi osobowymi*".
[36] art. 28 RODO.

3. Przetwarzanie przez podmiot przetwarzający powinno odbywać się na podstawie umowy[37] lub innego instrumentu prawnego, które podlegają prawu Unii Europejskiej lub prawu państwa członkowskiego i wiążą podmiot przetwarzający z ADO, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa Administratora; Umowa ta lub inny instrument prawny powinny stanowić w szczególności, że podmiot przetwarzający:
   1) przetwarza dane osobowe wyłącznie na udokumentowane polecenie ADO – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba, że obowiązek taki nakłada na niego prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje ADO o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;
   2) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
   3) podejmuje wszelkie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:
      a) pseudonimizację i szyfrowanie danych osobowych;
      b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
      c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
      d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
   4) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w art. 28 ust. 2 i 4 RODO;
   5) biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga ADO poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III Polityki;
   6) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga ADO wywiązać się z obowiązków zapewnienia bezpieczeństwa danych osobowych;
   7) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji ADO usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;

[37] Wzór - Załącznik **Nr 11a** do Polityki „*Umowa powierzenia przetwarzania danych osobowych*”.

8) udostępnia ADO wszelkie informacje niezbędne do wykazania spełnienia obowiązków oraz umożliwia Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich;
9) niezwłocznie informuje ADO, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie RODO lub innych przepisów Unii Europejskiej lub państwa członkowskiego o ochronie danych.

4. Jeżeli do wykonania w imieniu ADO konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii Europejskiej lub prawu państwa członkowskiego:
   1) te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między Administratorem, a podmiotem przetwarzającym, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom RODO;
   2) jeżeli ten inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na pierwotnym podmiocie przetwarzającym.
5. Bez uszczerbku dla indywidualnych umów pomiędzy ADO, a podmiotem przetwarzającym, umowa lub inny akt prawny, mogą się opierać w całości lub w części na standardowych klauzulach umownych także, gdy są one elementem certyfikacji udzielonej Administratorowi lub podmiotowi przetwarzającemu;
6. Umowa lub inny akt prawny, mają formę pisemną, w tym formę elektroniczną;
7. Jeżeli podmiot przetwarzający naruszy niniejsze postanowienia przy określaniu celów i sposobów przetwarzania, uznaje się go za Administratora w odniesieniu do tego przetwarzania.

§ 21.

W sytuacji powierzenia przetwarzania danych osobowych podmiotowi zewnętrznemu, w umowie powierzenia przetwarzania danych osobowych określa się przede wszystkim:
1) Cel i zakres przetwarzania danych osobowych;
2) Obowiązek zachowania w tajemnicy danych osobowych oraz informacji o zabezpieczeniach tych danych;
3) Konsekwencje prawne i kary finansowe wynikające z niestosowania się do warunków umowy;
4) Wymagania bezpieczeństwa dla procesu przetwarzania danych osobowych;
5) Spodziewany czas trwania umowy;
6) Wymagane działania w momencie zakończenia umowy;
7) Prawa do audytu i monitorowania działań związanych z ochroną danych osobowych;

8) Proces powiadamiania i raportowania nieuprawnionego ujawnienia lub naruszenia poufności i integralności danych osobowych;
9) Zasady zwrotu lub niszczenia danych osobowych przy zakończeniu umowy;
10) Działania podejmowane w przypadku naruszenia warunków umowy.

ROZDZIAŁ VI
REJESTROWANIE CZYNNOŚCI PRZETWARZANIA[38]

§ 22.

1. Administrator ma obowiązek prowadzenia *Rejestru Czynności Danych Osobowych*, za który odpowiada.
2. *Rejestr Czynności Przetwarzania Danych*[39] powinien zawierać nw. informacje:
   1) imię i nazwisko lub nazwę oraz dane kontaktowe ADO oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela Administratora oraz inspektora ochrony danych;
   2) cele przetwarzania;
   3) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
   4) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
   5) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej;
   6) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
   7) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.
3. Podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego mają obowiązek prowadzić *Rejestr wszystkich kategorii czynności przetwarzania*[40], dokonywanych w imieniu Administratora, zawierający następujące informacje:
   1) imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych;
   2) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
   3) gdy ma to zastosowanie – przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej;
   4) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.
4. Rejestry, o których mowa w ust. 2 i 3, mają formę pisemną, w tym formę elektroniczną.

[38] art. 30 ust. 1 RODO.
[39] Wzór - Załącznik **Nr 12** do Polityk „*Rejestr czynności przetwarzania danych osobowych*".
[40] Wzór - Załącznik **Nr 13** do Polityki „*Rejestr wszystkich kategorii czynności przetwarzania*".

5. Administrator lub podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel administratora lub podmiotu przetwarzającego udostępniają rejestr na żądanie organu nadzorczego.

ROZDZIAŁ VII
ŚRODKI TECHNICZNE I ORGANIZACYJNE ZAPEWNIAJĄCE STOPIEŃ BEZPIECZEŃSTWA[41]

A. BEZPIECZEŃSTWO PRZETWARZANIA

§ 23.

1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, Administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:
   1) pseudonimizację i szyfrowanie danych osobowych;
   2) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów usług przetwarzania;
   3) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
   4) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania;
   5) inwentaryzację zbiorów danych osobowych[42] oraz inwentaryzację zasobów[43]:
      a) obszary przetwarzania (siedziba organizacji) – pomieszczenia, w których przetwarzane są dane osobowe z uwzględnieniem lokalizacji, zasilania w energię elektryczną i sposobu jej rozprowadzenia, dostępu do usług telekomunikacyjnych, stref o różnych poziomach dostępu, lub istotności przetwarzanych danych (np. pomieszczenia, w których znajduje się sprzęt komputerowy oraz te, w których go nie ma);
      b) sieć teleinformatyczna – architektura sieci z uwzględnieniem sposobu jej rozprowadzenia (np. Ethernet, Wi-Fi, ADSL, wydzielone warstwy), użytych urządzeń pośredniczących (switch, router, hub itp.), a także innych urządzeń i rozwiązań zastosowanych przez administratora;
      c) sprzęt – serwery, komputery stacjonarne, komputery i inne urządzenia przenośne, nośniki danych, drukarki;
      d) oprogramowanie – począwszy od systemów operacyjnych (Windows, Linux), poprzez programy wspomagające zarządzanie (antywirus, firewall, zarządzanie kontami użytkowników,

[41] art. 32 RODO.
[42] Wzór - Załącznik **Nr 10** do Polityki „*Inwentaryzacja zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych”.*
[43] Wzór - Załącznik **Nr 15** do Polityki „*Inwentaryzacja zasobów*”.

oprogramowanie monitorujące) oraz programy użytkowe i aplikacje biznesowe (edytory tekstu, arkusze kalkulacyjne, komunikatory, przeglądarki, programy pocztowe, programy księgowe, programy magazynowe, programy graficzne, projektowe, itd.); należy pamiętać o dwóch kwestiach: inwentaryzacja oprogramowania musi objąć również oprogramowanie bezpłatne, a także do każdego programu powinniśmy posiadać licencję, aby zapewnić legalność jego użytkowania;

e) personel – pracownicy z podziałem na funkcje (menadżerowie, pracownicy przetwarzający dane osobowe, obsługa techniczna, itp.), podmioty i osoby współpracujące na zasadach umów cywilnoprawnych, które przetwarzają lub mają wpływ na przetwarzanie danych osobowych w organizacji;

f) inne nośniki danych – teczki spraw, umowy, akta osobowe, książki adresowe, skorowidze zawierające dane osobowe itp.

2. Oceniając czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

3. Administrator oraz podmiot przetwarzający podejmują działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo Unii Europejskiej lub prawo państwa członkowskiego, stanowią o tym odrębne przepisy określone w „*Instrukcji zarządzania systemem informatycznym*”[44].

B. ODPOWIEDZIALNOŚĆ PRACOWNIKÓW W ZAKRESIE OCHRONY DANYCH OSOBOWYCH

§ 24.

1. Niezastosowanie się przez pracowników do przepisów prawa powszechnie obowiązującego oraz wprowadzonych zasad i procedur ochrony danych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 § 1 Kodeksu Pracy[45].

2. Niezależnie od rozwiązania stosunku pracy osoby dokonujące naruszenia mogą być pociągane do odpowiedzialności karnej zwłaszcza na podstawie art. 107 ustawy oraz art. 266 Kodeksu karnego[46], m.in. przestępstwo można popełnić wskutek:

[44] Załącznik Nr 2 do Zarządzenia Nr ..... Dyrektora Gminnego Centrum Kultury i Sportu w Ostrowie z/s w Kamionce z dn. ..... r. - „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Gminnym Centrum Kultury i Sportu w Ostrowie z/s w Kamionce”.
[45] ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz. U. z 2020 r. poz. 1320 ze zm.)
[46] ustawa z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz. U. z 2020 r. poz. 1444 ze zm.)

1) stworzenia możliwości dostępu do danych osobowych osobom nieupoważnionym albo osobie nieupoważnionej;
2) niezabezpieczenia nośnika lub komputera przenośnego przed dostępem osób upoważnionych;
3) zapoznania się z hasłem innego pracownika wskutek wykonania nieuprawnionych operacji w systemie informatycznym administratora danych;
4) pozostawienia osoby nieupoważnionej w pomieszczeniu biurowym, w którym przetwarzane są dane osobowe;
5) pozostawiania po godzinach pracy w pomieszczeniach biurowych, do których dostęp mają osoby nieupoważnione, dokumentów niezabezpieczonych przed ich dostępem.

3. Zgodnie z art. 100 § 2 pkt 5 Kodeksu Pracy, pracownik jest obowiązany przestrzegać tajemnicy określonej w odrębnych przepisach.

4. Pracownik dopuszczający się nieuprawnionego ujawnienia lub wykorzystania danych osobowych w sposób sprzecznych z ich przeznaczeniem (np. wykorzystania danych osobowych do celów prywatnych), czy też ich przetwarzania w sposób niezgodny z przyjętymi zasadami i procedurami może zostać ukarany karą upomnienia lub karą nagany.

5. W razie ciężkiego naruszenia obowiązku zachowania danych osobowych w tajemnicy lub przetwarzania ich w sposób rażąco sprzeczny z przyjętymi zasadami i procedurami, administrator może rozwiązać bez wypowiedzenia umowę o pracę z winy pracownika.

C. ZOBOWIĄZANIE UŻYTKOWNIKÓW

§ 25.

1. W celu osiągnięcia i utrzymania wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych konieczne jest zaangażowanie ze strony każdego użytkownika w zakresie ochrony danych osobowych.

2. Użytkownicy zobowiązani są do informowania IOD o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane.

3. Użytkownicy przede wszystkim zobowiązani są do:
   1) postępowania zgodnie z *Polityką* i dokumentami powiązanymi;
   2) zachowania w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia;
   3) ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem;
   4) wykonywania konkretnych działań i procesów, w celu zapewnienia ochrony danych osobowych.

4. Użytkownicy powinni mieć świadomość możliwości zaistnienia sytuacji naruszenia ochrony danych osobowych. W tym celu powinni:

1) przestrzegać procedur związanych z otwieraniem i zamykaniem pomieszczeń, a także z wejściem do obszarów przetwarzania danych osobowych osób nieupoważnionych;
2) informować ADO o podejrzanych osobach przebywających w rejonie miejsca, w którym przetwarzane są dane osobowe;
3) użytkownicy powinni na podstawie dokonanej identyfikacji ewentualnych zagrożeń, przedkładać IOD projekty i propozycje nowych rozwiązań, których celem jest zwiększenie poziomu ochrony danych osobowych.

§ 26.

1. Użytkownicy w celu ochrony informacji dotyczących danych osobowych powinni podczas przetwarzania uwzględniać następujące zasady:
   1) wykorzystywania techniki kryptograficznej do ochrony poufności, integralności i rozliczalności danych osobowych przetwarzanych poza siedzibą organizacji;
   2) ochrony danych osobowych przed przechwyceniem, kopiowaniem, modyfikacją oraz błędnym wyborem drogi komunikacji i zniszczeniem;
   3) stosowania zabezpieczenia i ograniczenia związane z możliwościami przekazywania wiadomości za pomocą środków komunikacji, np. automatyczne przekazywania poczty elektronicznej na zewnątrz organizacji;
   4) nie pozostawiania informacji zawierających dane osobowe przy urządzeniach drukujących, np. kserokopiarkach, drukarkach, faksach, do których mogą mieć dostęp osoby nieupoważnione;
   5) upewnienia się przed przekazaniem danych osobowych, czy rozmówca jest osobą upoważnioną do uzyskania określonych danych osobowych;
   6) zachowania szczególnej ostrożności w trakcie rozmów telefonicznych, unikając podsłuchania danych osobowych przez osoby nieupoważnione;
   7) nie pozostawiania wiadomości zawierających dane osobowe w automatycznych sekretarkach, a także w serwisach internetowych (bez zgody osoby, której dane są przetwarzane).
2. Transport danych osobowych w formie elektronicznej i papierowej pomiędzy obszarami, w których są przetwarzane dane osobowe powinien być prowadzony przez osoby upoważnione w sposób ograniczający możliwość ich pozyskania i odczyt przez osoby nieupoważnione.

§ 27.

1. Zastosowane rozwiązania techniczne umożliwiające dostęp zdalny do danych osobowych powinny zapewniać integralność, poufność i rozliczalność przetwarzanych danych osobowych oraz ochronę kryptograficzną wobec danych służących do uwierzytelnia, a przesyłanych publicznymi łączami telekomunikacyjnymi.

2. Nadawanie uprawnień w celu dostępu zdalnego do systemów informatycznych przetwarzających dane osobowe realizowane powinno być realizowane przez ASI, po spełnieniu wymagań określonych w ust. 1 oraz po uzyskaniu akceptacji ADO.
3. Dostęp do systemów informatycznych dla użytkowników zewnętrznych powinien być monitorowany pod kątem bezpieczeństwa przez ASI, w celu zapewnienia poufności, rozliczalności i integralności danych osobowych.

§ 28.

1. Zbiory w systemie tradycyjnym powinny być odpowiednio zabezpieczone przed nieuprawnionym dostępem i zniszczeniem.
2. Dokumenty i wydruki zawierające dane osobowe, należy przechowywać w zamykanych pomieszczeniach, do których dostęp mają jedynie uprawnione osoby.
3. Na czas nieużytkowania, dokumenty i wydruki zawierające dane osobowe powinny być umieszczane w szafach biurowych, szufladach bądź pomieszczeniach zamykanych na klucz tak, aby ograniczyć do nich dostęp osobom nieuprawnionym.
4. Wydruki robocze, błędne lub zdezaktualizowane powinny być niezwłocznie niszczone przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie lub zanonimizowanie.
5. Dla udokumentowania czynności dokonywanych w celu likwidacji zbiorów archiwalnych, powinny być stosowane przepisy wykonawcze do ustawy o narodowym zasobie archiwalnym i archiwach[47] .

§ 29.

1. Na stacjach roboczych powinno być zainstalowane jedynie oprogramowanie niezbędne do pracy, na które administrator posiada ważne licencje.
2. Inwentaryzacja oprogramowania zainstalowanego na stacjach roboczych powinna być prowadzona na bieżąco.
3. Po zakończeniu pracy użytkownik powinien wyłączyć użytkowany komputer.

§ 30.

Ścisłe zasady archiwizacji danych w systemie informatycznym:

1) archiwizacja danych przeprowadzona jest indywidualnie przez każdego z uprawnionych użytkowników;

[47] Rozporządzenie Ministra Kultury i Dziedzictwa Narodowego z dnia 20 października 2015 r. *w sprawie klasyfikowania i kwalifikowania dokumentacji, przekazywania materiałów archiwalnych do archiwów państwowych i brakowania dokumentacji niearchiwalnej* (Dz.U. 2015 poz. 1743 ze zm.).

2) kopie zapasowe przechowywane powinny być w miejscu zabezpieczonym przed dostępem osób nieupoważnionych, a poza budynkami Gminnego Centrum Kultury i Sportu w Ostrowie, również w formie zaszyfrowanej;
3) ADO oraz ASI nie mają obowiązku tworzenia backupów danych osobowych, zapisanych na nośnikach elektronicznych użytkowanych przez poszczególne osoby upoważnione.

§ 31.

Ochrona antywirusowa powinna być prowadzona według poniższych zasad:

1) na wszystkich stacjach roboczych i serwerach instalowane jest oprogramowanie antywirusowe z wyjątkiem urządzeń, których budowa uniemożliwia instalowanie bądź zmianę kodów źródłowych oprogramowania;
2) konfiguracja oprogramowania może być zmieniana jedynie przez upoważnione osoby;
3) użytkownik nie może deinstalować ani wyłączać oprogramowania antywirusowego;
4) wszystkie pliki wprowadzone do systemu z nośników zewnętrznych w szczególności tj. optyczne nośniki danych, pendrive, dyski twarde, karty pamięci, a także pobierane z sieci Internet, muszą być wcześniej sprawdzone przez oprogramowanie antywirusowe (manualnie bądź poprzez zautomatyzowane mechanizmy oprogramowania antywirusowego);
5) wiadomości pocztowe przed otwarciem powinny być na bieżąco monitorowane przez oprogramowanie antywirusowe.

§ 32.

Zabezpieczenia fizyczne:

1) sprzęt komputerowy powinien znajdować się w zabezpieczonych pomieszczeniach;
2) każde pomieszczenie, w którym przechowuje się dane osobowe powinno być zamykane na klucz, jeśli upoważniona osoba w nim nie przebywa;
3) osoby nieupoważnione nie mogą przebywać bez nadzoru w pomieszczeniach, w których przetwarzane są dane osobowe;
4) w pomieszczeniach, w których znajduje się sprzęt komputerowy, obowiązuje zakaz używania otwartego ognia oraz palenia tytoniu;
5) ekrany monitorów należy ustawić w taki sposób, aby uniemożliwić odczyt treści wyświetlanych na ekranie osobom nieupoważnionym.

D. ZABEZPIECZENIE SYSTEMÓW INFORMATYCZNYCH

§ 33.

1. Przed atakami z sieci zewnętrznej wszystkie komputery chronione są środkami dobranymi przez ASI w porozumieniu z IOD oraz ADO.
2. Użytkownicy zobowiązani są do zwracania uwagi na to czy urządzenie, na którym pracują domaga się aktualizacji zabezpieczeń.
3. Zabrania się stosowania opcji „zapamiętywania haseł" przez użytkowane przeglądarki internetowe.
4. O wszystkich przypadkach wskazujących na utratę danych należy informować IOD lub ASI oraz umożliwić im monitorowanie i aktualizację środków bezpieczeństwa.
5. ASI w porozumieniu z IOD dobiera elektroniczne środki ochrony przed atakami z sieci stosownie do pojawiania się nowych zagrożeń, a także stosownie do rozbudowy systemu informatycznego administratora i rozbudowy bazy danych.
6. Należy zwracać uwagę, czy rozwijający się system zabezpieczeń sam nie wywołuje nowych zagrożeń.
7. Należy stosować następujące sposoby kryptograficznej ochrony danych:
   1) przy przesyłaniu danych za pomocą poczty elektronicznej stosuje się „POP" – tunelowanie, szyfrowanie połączenia;
   2) przy przesyłaniu danych pracowników niezbędnych do wykonania przelewów wynagrodzeń, używa się zabezpieczonych stron internetowych.

§ 34.

1. System informatyczny posiada szerokopasmowe połączenie z Internetem.
2. Użytkownicy zobowiązani są korzystać tylko z bezpiecznych połączeń internetowych (zabrania się korzystania z tzw. hot spotów i niezabezpieczonych sieci publicznych).
3. Korzystanie z zasobów sieci wewnętrznej jest możliwe tylko w zakresie uprawnień przypisanych do danego konta osoby upoważnionej do przetwarzania danych osobowych.
4. Operacje za pośrednictwem rachunku bankowego ADO może wykonywać wyłącznie upoważniony pracownik księgowości, po uwierzytelnieniu się zgodnie z procedurami określonymi przez bank obsługujący rachunek.

§ 35.

1. Dane osobowe mogą być przetwarzane wyłącznie w budynkach i pomieszczeniach wyznaczonych do przetwarzania danych osobowych.

2. Do pomieszczeń przetwarzania danych osobowych zalicza się pomieszczenia[48]:
   1) serwerowni,
   2) biurowe:
      a) zlokalizowane są stacje robocze,
      b) przechowywane są sprawne oraz uszkodzone elektroniczne nośniki informacji, kopie zapasowe,
      c) przechowuje się dokumenty źródłowe oraz wydruki z systemu informatycznego,
      d) zlokalizowane są zbiory nieinformatyczne,
      e) archiwizuje się dane osobowe.
3. Nośniki elektroniczne zawierające dane osobowe powinny być ewidencjonowane i przechowywane w zamykanych szafach, które znajdują się w obszarach przetwarzania danych osobowych.
4. W przypadkach szczególnie uzasadnionych, jeżeli wymaga tego charakter powierzonych zadań i obowiązków, dopuszcza się również możliwość przetwarzania danych osobowych poza siedzibą GCKiS.

E. NARUSZENIE OCHRONY DANYCH OSOBOWYCH

§ 36.

1. Postanowienia *Polityki* mają zastosowanie zarówno w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych przetwarzanych w systemach informatycznych oraz w systemach tradycyjnych.
2. Za okoliczności, które uznaje się za naruszenie lub podejrzenie naruszenia ochrony systemu przetwarzającego dane osobowe, uważa się w szczególności:
   1) nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one przetwarzane;
   2) nieuprawnione naruszenie lub próby naruszenia poufności, integralności i rozliczalności danych i systemu;
   3) niezamierzoną zmianę lub utratę danych zapisanych na kopiach zapasowych;
   4) nieuprawniony dostęp do danych osobowych (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu informatycznego);
   5) udostępnienie osobom nieupoważnionym danych osobowych bądź haseł użytkowników;
   6) inny stan systemu informatycznego lub pomieszczeń, niż pozostawiony przez użytkownika po zakończeniu pracy;
   7) wydarzenia losowe obniżające poziom ochrony systemu (np. brak zasilania, niesprawne ogrzewanie CO w okresie zimowym lub pożar);

[48] Wzór - Załącznik **Nr 14** do Polityki „Wykaz budynków i pomieszczeń, w których przetwarzane są dane osobowe".

8) kradzież sprzętu informatycznego lub nośników zewnętrznych zawierających dane osobowe (np. wydruków komputerowych, płyt CD lub DVD, dysków twardych, pamięci zewnętrznych, itp.).

3. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych pracownicy zobowiązani są do bezzwłocznego powiadomienia o tym fakcie ADO oraz IOD.

4. ADO zobowiązany jest ocenić czy zachodzą przesłanki do zgłoszenia naruszenia PUODO oraz powiadomienia osoby, której dane dotyczą o naruszeniu.

5. Szczegółowy sposób postępowania w sytuacji naruszenia ochrony danych osobowych reguluje „*Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych w Gminnym Centrum Kultury i Sportu w Ostrowie z/s w Kamionce*”[49].

F. OCENA SKUTKÓW DLA OCHRONY DANYCH[50]

§ 37.

1. Jeżeli rodzaj danych ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, ADO przed rozpoczęciem przetwarzania powinien dokonać oceny skutków[51] planowanych operacji przetwarzania dla ochrony danych osobowych.

2. Dokonując oceny skutków dla ochrony danych, ADO powinien skonsultować się z IOD.

3. Ocena skutków dla ochrony danych, o której mowa w ust. 1, jest wymagana w szczególności w przypadku:
   1) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
   2) przetwarzania na dużą skalę szczególnych kategorii danych osobowych[52].

4. Ocena zawiera co najmniej:
   1) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, 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;

[49] Załącznik Nr 3 do Zarządzenia Nr ..... Dyrektora Gminnego Centrum Kultury i Sportu w Ostrowie z/s w Kamionce z dn. ..... r. - „Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych w Gminnym Centrum Kultury i Sportu w Ostrowie z/s w Kamionce”.
[50] art. 35 RODO.
[51] Wzór Załącznik **Nr 5** do *Polityki* „*Ocena skutków naruszenia*”.
[52] art. 8 RODO.

4) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą oraz innych osób, których sprawa dotyczy.

5. W stosownych przypadkach ADO zasięga opinii osób, których dane dotyczą lub ich przedstawicieli, w sprawie zamierzonego przetwarzania bez uszczerbku dla ochrony interesów handlowych lub publicznych albo bezpieczeństwa operacji przetwarzania.

6. W razie potrzeby przynajmniej, gdy zmienia się ryzyko wynikające z operacji przetwarzania, ADO dokonuje przeglądu, aby stwierdzić czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych.

ROZDZIAŁ VIII
ZAKRES KOMPETENCJI

A. KOMPETENCJE ADMINISTRATORA DANYCH OSOBOWYCH

§ 38.

1. W celu zwiększenia skuteczności ochrony danych osobowych w zależności od potrzeb ADO powinien stosować nw. założenia:
   1) przeszkolenie pracowników dopuszczonych do przetwarzania w zakresie bezpieczeństwa danych osobowych;
   2) przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację w systemach informatycznych (np. hasła, identyfikatory), umożliwiających im dostęp do danych osobowych stosownie do zakresu upoważnienia i indywidualnych poziomów uprawnień;
   3) okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych;
   4) podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie ochrony danych osobowych;
   5) monitorowanie osiągnięć w dziedzinie bezpieczeństwa systemów informatycznych i w miarę możliwości organizacyjnych oraz techniczno-finansowych, wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania systemami informatycznymi, służącym wzmocnieniu bezpieczeństwa przetwarzanych danych osobowych.

2. ADO powinien być pewny, że pracownicy, kontrahenci oraz użytkownicy zewnętrzni:
   1) przed przystąpieniem do pracy są odpowiednio wprowadzani w zakres obowiązków związanych z odpowiedzialnością przestrzegania ochrony danych osobowych przy przetwarzaniu danych;
   2) wypełniają zalecenia i warunki zatrudnienia, które uwzględniają zasady ochrony danych osobowych;

3) w sposób ciągły utrzymują odpowiednie umiejętności i kwalifikacje.

3. ADO powinien też zapewnić zgodność postępowania kontrahentów z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych.

§ 39.

1. Do kompetencji ADO w szczególności należy:
   1) wyznaczenie IOD;
   2) wyznaczenie ASI;
   3) określenie celów i strategii ochrony danych osobowych;
   4) podział zadań i obowiązków związanych z organizacją ochrony danych osobowych.
2. Do obowiązków ADO należy:
   1) przyjmowanie i zatwierdzanie niezbędnych, wymaganych przez przepisy prawa dokumentów regulujących ochronę danych osobowych;
   2) zapewnienie środków finansowych na ochronę fizyczną pomieszczeń, w których przetwarzane są dane osobowe;
   3) zapewnienie środków finansowych niezbędnych do ochrony danych osobowych przetwarzanych w systemie tradycyjnym oraz w systemach informatycznych;
   4) zapewnienie środków finansowych na merytoryczne przygotowanie osób odpowiedzialnych za nadzór nad ochroną danych osobowych.

§ 40.

1. ADO wyznacza inspektora ochrony danych[53].
2. IOD jest wyznaczany na podstawie kwalifikacji zawodowych, w szczególności na podstawie wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań[54].
3. ADO ma obowiązek opublikować dane kontaktowe IOD i zawiadomić o nim organ nadzorczy.

§ 41.

1. ADO powinien zapewnić, by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
2. ADO powinien wspierać IOD w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.

[53] art. 39 RODO.
[54] art. 39 RODO.

3. ADO powinien zapewnić by IOD nie otrzymywał instrukcji dotyczących wykonywania tych zadań.
4. IOD nie może być odwołany ani karany przez ADO za wypełnianie swoich zadań, pod warunkiem, iż jego działania nie wiążą się z naruszeniem przepisów prawa.
5. Osoby, których dane dotyczą, mogą kontaktować się z IOD we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia.
6. IOD jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii Europejskiej lub prawem państwa członkowskiego.

B. KOMPETENCJE INSPEKTORA OCHRONY DANYCH (IOD)[55]

§ 42.

1. Do zadań IOD należy[56]:
   1) bieżące informowanie ADO, podmiotu przetwarzającego oraz pracowników GCKiS, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy przepisów RODO oraz innych przepisów Unii Europejskiej lub krajowych w zakresie ochrony danych osobowych i doradzanie w przedmiotowym zakresie;
   2) monitorowanie przestrzegania przepisów RODO, innych przepisów Unii Europejskiej lub krajowych o ochronie danych osobowych oraz *Polityki* ADO w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz wykonywanie okresowych audytów;
   3) udzielanie zaleceń co do oceny skutków dla ochrony danych osobowych oraz monitorowanie jej wykonania;
   4) współpraca z organem nadzorczym;
   5) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;
   6) reagowanie w sytuacji podejrzenia incydentów związanych z ochroną danych osobowych;
   7) konsultacje umów powierzenia przetwarzania danych osobowych oraz pomoc w opracowywaniu treści klauzul informacyjnych oraz zgód na przetwarzanie danych osobowych,
   8) pomoc w utrzymaniu i aktualizacji dokumentacji tj. polityk, procedur i rejestrów związanych z przetwarzaniem danych osobowych.

[55] art. 39 RODO.
[56] Załącznik Nr 5 do Zarządzenia Nr ..... Dyrektora Gminnego Centrum Kultury i Sportu w Ostrowie z/s w Kamionce z dn. ..... r. - „*Regulamin funkcjonowania Inspektora Ochrony Danych w Gminnym Centrum Kultury i Sportu w Ostrowie z/s w Kamionce*”.

2. IOD wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania danych osobowych mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

C. KOMPETENCJE ADMINISTRATORA SYSTEMU INFORMATYCZNEGO (ASI)

§ 43.

1. ADO powołuje Administratora Systemu Informatycznego.
2. Do kompetencji ASI należy:
   1) zabezpieczenie systemów przetwarzania danych osobowych zgłoszonych ASI, w zależności od kategorii przetwarzanych w tym systemie danych;
   2) zapewnienie poufności, integralności, dostępności i rozliczalności danych przetwarzanych w systemach informatycznych.
3. Do obowiązków ASI należy:
   1) nadzór oraz zapewnianie optymalnej ciągłości działania systemu informatycznego, w tym pomoc w opracowaniu procedur określających zarządzanie systemem informatycznym przetwarzającym dane osobowe;
   2) reagowanie bez zbędnej zwłoki, w przypadku naruszenia bądź powstania zagrożenia bezpieczeństwa danych osobowych;
   3) przeciwdziałanie próbom naruszenia bezpieczeństwa danych osobowych poprzez stosowanie oprogramowania antywirusowego, a także konfigurację zabezpieczeń sieciowych;
   4) analiza raportów zdarzeń związanych z bezpieczeństwem systemów przetwarzania danych;
   5) zapewnienie zgodności wdrażanych systemów przetwarzania danych osobowych z RODO oraz z „Polityką” i „Instrukcją zarządzania systemem informatycznym”, w tym opiniowanie w zakresie planowanego wdrożenia oprogramowania informatycznego;
   6) w porozumieniu z ADO, instalacja i konfiguracja oprogramowania oraz sprzętu teleinformatycznego sieciowego do przetwarzania danych osobowych;
   7) konfiguracja i administracja oprogramowaniem systemowym i sieciowym, zabezpieczającym dane osobowe przed nieupoważnionym dostępem;
   8) nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności szkodliwego oprogramowania;
   9) nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji;
   10) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe;
   11) przyznawanie na wniosek ADO ściśle określonych praw dostępu do danych osobowych w danym systemie;

12) świadczenie pomocy technicznej w ramach oprogramowania, a także serwis sprzętu komputerowego będącego na stanie, służącego do przetwarzania danych osobowych;
13) diagnozowanie i usuwanie awarii sprzętu komputerowego oraz pomoc przy realizacji umów z firmami świadczącymi usługi napraw pogwarancyjnych sprzętu informatycznego;
14) wykonywanie i zarządzanie kopiami zapasowymi oprogramowania systemowego i sieciowego;
15) nadzór nad wdrożeniem i zarządzanie aplikacjami, w których przetwarza się dane osobowe, w zakresie wynikającym z zawartej umowy z ADO.

4. Obowiązki, o których mowa w ust. 3, mogą być realizowane przez ASI również przy pomocy szyfrowanych, zdalnych kanałów komunikacji. Odpowiedzialność za bezpieczeństwo przeprowadzanych zdalnych połączeń z systemem informatycznym ponosi ASI. ASI jest zobowiązany do informowania ADO o planowanych działaniach z wykorzystaniem zdalnych kanałów komunikacji.

§ 44.

1. Przed rozpoczęciem przetwarzania danych osobowych, pracownik powinien zostać zapoznany z przepisami o ochronie danych osobowych, w tym obowiązującymi procedurami w tym zakresie, a także przeszkolony z ochrony danych osobowych.
2. Szkolenie, o którym mowa w ust. 1 powyżej, powinno obejmować następujące zagadnienia:
   1) przepisy o ochronie danych osobowych;
   2) zasady przetwarzania danych osobowych;
   3) procedury dotyczące bezpiecznego przetwarzania danych osobowych w systemach Informatycznych;
   4) zasady użytkowania urządzeń i systemów informatycznych służących do przetwarzania danych osobowych;
   5) zagrożenia na jakie może być narażone przetwarzanie danych osobowych, a w szczególności związane z przetwarzaniem danych osobowych w systemach informatycznych;
   6) zasady dostępu do pomieszczeń, w których przetwarzane są dane osobowe;
   7) sposób postępowania w przypadku naruszenia ochrony danych osobowych lub systemu informatycznego;
   8) odpowiedzialność z tytułu naruszenia ochrony danych osobowych.
3. Szkolenia powinny być powtarzane okresowo lub na żądanie.

ROZDZIAŁ IX
POSTANOWIENIA KOŃCOWE

§ 45.

1. „Polityka” powinna być poddawana weryfikacji przynajmniej raz na rok pod kątem:

1) zmian w strukturze systemu informatycznego;
2) zmian organizacyjnych ADO, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych;
3) zmian w obowiązującym prawie.

2. Przeglądu „Polityki” dokonuje ADO, biorąc pod uwagę zalecenia i wnioski ASI oraz IOD.
3. ADO danych biorąc pod uwagę wnioski IOD, może zlecić przeprowadzenie audytu zewnętrznego przez wyspecjalizowany podmiot.

§ 46.

Osobom przeszkolonym może zostać przekazany wyciąg z Polityki oraz dokumentów powiązanych, z uwzględnieniem obowiązków dotyczących ochrony danych osobowych na poszczególnych stanowiskach.

ZAŁĄCZNIKI: WZORY DO *POLITYKI*

1) Załącznik **Nr 1** do Polityki „*Oświadczenie osoby wyrażającej zgodę na przetwarzanie jej danych osobowych*”
2) Załącznik **Nr 2** do Polityki „*Informacja o zbieraniu danych osobowych od osoby, której dane dotyczą*”
3) Załącznik **Nr 3** do Polityki „*Informacja o zbieraniu danych osobowych nie od osoby, której dane dotyczą*”
4) Załącznik **Nr 4** do Polityki „*Informacja o przetwarzaniu danych osobowych*”
5) Załącznik **Nr 5** do Polityki „*Ocena skutków naruszenia*”
6) Załącznik **Nr 6** do Polityki „*Ocena ryzyka naruszenia*”
7) Załącznik **Nr 7** do Polityki „*Lista osób uczestniczących w szkoleniu z zakresu ochrony danych osobowych*”
8) Załącznik **Nr 8** do Polityki „*Ankieta sprawdzenia wiedzy pracownika z zakresu ochrony danych osobowych*”
9) Załącznik **Nr 9** do Polityki „*Raport sprawdzenia zgodności z przepisami ochrony danych osobowych*”
10) Załącznik **Nr 10** do Polityki ”*Inwentaryzacja zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych*”
11) Załącznik **Nr 11** do Polityki „*Rejestr umów powierzenia przetwarzania danych*”
12) Załącznik **Nr 11a** do Polityki „*Umowa powierzenia przetwarzania danych osobowych*”
13) Załącznik **Nr 11b** do Polityki „*Umowa pomiędzy współadministratorami*”
14) Załącznik **Nr 12** do Polityki „*Rejestr czynności przetwarzania danych osobowych*”
15) Załącznik **Nr 13** do Polityki „*Rejestr wszystkich kategorii czynności przetwarzania*”
16) Załącznik **Nr 14** do Polityki „*Wykaz budynków i pomieszczeń, w których przetwarzane są dane osobowe”*
17) Załącznik **Nr 15** do Polityki „*Inwentaryzacja zasobów”.*

WZÓR

ZAŁĄCZNIK NR 1 DO
POLITYKI BEZPIECZEŃSTWA

OŚWIADCZENIE OSOBY WYRAŻAJĄCEJ ZGODĘ NA PRZETWARZANIE JEJ DANYCH OSOBOWYCH

Oświadczam, iż wyrażam zgodę na przetwarzanie moich danych osobowych przez ..... na podstawie art. 6 ust. 1 lit. a RODO / art. 9 ust. 2 lit. a RODO w celu .....

.....
(data, podpis)

Zgodnie z art. 13 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 informujemy, że:

1. Administratorem Pani/Pana* danych osobowych jest ..... dane kontaktowe .....
2. Inspektorem ochrony danych jest ....., dane kontaktowe[57] .....
3. Pani/Pana* dane osobowe przetwarzane będą w celu[58] ..... na podstawie[59] .....
4. Odbiorcą Pani/Pana* danych osobowych będą[60] .....
5. Pani/Pana* dane osobowe będą przechowywane przez okres[61] .....
6. Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania[62], którego dokonano na podstawie zgody przed jej cofnięciem;
7. Posiada Pani/Pan prawo wniesienia skargi do PUODO gdy uzna Pani/Pan, iż przetwarzanie danych osobowych dot. narusza przepisy RODO.
8. Podanie przez Panią/Pana* danych osobowych jest[63] ..... Jest Pani/Pan* zobowiązana do ich podania, a konsekwencją niepodania danych osobowych będzie[64]: .....
9. Pani/Pana* dane będą/nie będą* podlegać zautomatyzowanemu podejmowaniu decyzji, w tym również profilowaniu. Zautomatyzowane podejmowanie decyzji będzie odbywało się na zasadach: ..... konsekwencją takiego przetwarzania będzie[65]: .....

Potwierdzam zapoznanie się z treścią powyższej klauzuli informacyjnej

.....
(data, podpis)

[57] e-mail lub inne dane kontaktowe.
[58] należy podać cel przetwarzania.
[59] należy podać podstawę prawną przetwarzania np. art. 6 ust 1 pkt a/b/c/d/e/f. *Przy podpunkcie f należy wskazać uzasadniony interes ADO lub strony trzeciej.
[60] można wymienić kategorię odbiorców o ile istnieją.
[61] jeżeli nie ma możliwości wskazania okresu przechowywania należy podać kryterium ustalania tego okresu np. do czasu wyłonienia zwycięzcy konkursu, do czasu zakończenia rekrutacji itd.
[62] jeżeli przetwarzanie odbywa się na podstawie zgody.
[63] wybrać odpowiednio: wymogiem ustawowym/warunkiem umownym/warunkiem zawarcia umowy.
[64] jeżeli osoba, której dane dotyczą, jest zobowiązana do ich podania należy wskazać ewentualne konsekwencje niepodania danych.
[65] należy wskazać istotne informacje o zasadach zautomatyzowanego podejmowania decyzji oraz informacje o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą. Np. w jaki sposób będą oceniane czynniki osobowe osoby fizycznej, natomiast przykładową konsekwencją takiego przetwarzania może być automatyczne odrzucenie elektronicznego wniosku kredytowego czy elektroniczne metody rekrutacji bez interwencji ludzkiej

WZÓR

ZAŁĄCZNIK NR 2 DO
POLITYKI BEZPIECZEŃSTWA

INFORMACJE O ZBIERANIU DANYCH OSOBOWYCH OD OSOBY, KTÓREJ DOTYCZĄ

Na podstawie art. 14 ust. 1 i 2 rozporządzenia[66] ..... informuje, że:

1. Administratorem Pani/Pana* danych osobowych jest .....

   dane kontaktowe .....
2. Inspektorem ochrony danych jest ....., dane kontaktowe[67]

   .....
3. Pani/Pana* dane osobowe przetwarzane będą w celu[68] .....
   na podstawie[69] .....
4. Odbiorcą Pani/Pana* danych osobowych będą[70] .....
5. Pani/Pana* dane osobowe będą przechowywane przez okres[71] .....
6. Posiada Pani/Pan* prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania[72],
7. Ma Pani/Pana* prawo wniesienia skargi do PUODO gdy uzna Pani/Pan*, iż przetwarzanie danych osobowych dotyczących Pani/Pana osoby narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.
8. Podanie przez Panią/Pana* danych osobowych jest[73] .....

   Jest Pani/Pan* zobowiązana do ich podania, a konsekwencją niepodania danych osobowych będzie[74]:

   .....

   .....
9. Pani/Pana* dane będą/ nie będą* podlegać zautomatyzowanemu podejmowaniu decyzji, w tym również profilowaniu. Zautomatyzowane podejmowanie decyzji będzie odbywało się na zasadach: .....

   .....

   konsekwencją takiego przetwarzania będzie[75]: .....

.....
Administrator Danych Osobowych

* niepotrzebne skreślić

[66] 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.

[67] e-mail lub inne dane kontaktowe.

[68] należy podać cel przetwarzania.

[69] należy podać podstawę prawną przetwarzania np. art. 6 ust 1 pkt a/b/c/d/e/f. *Przy podpunkcie f należy wskazać uzasadniony interes ADO lub strony trzeciej.

[70] można wymienić kategorię odbiorców o ile istnieją.

[71] jeżeli nie ma możliwości wskazania okresu przechowywania należy podać kryterium ustalania tego okresu np. do czasu wyłonienia zwycięzcy konkursu, do czasu zakończenia rekrutacji itd.

[72] jeżeli przetwarzanie odbywa się na podstawie zgody.

[73] wybrać odpowiednio: wymogiem ustawowym/warunkiem umownym/warunkiem zawarcia umowy.

[74] jeżeli osoba, której dane dotyczą, jest zobowiązana do ich podania należy wskazać ewentualne konsekwencje niepodania danych.

[75] należy wskazać istotne informacje o zasadach zautomatyzowanego podejmowania decyzji oraz informacje o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą. Np. w jaki sposób będą oceniane czynniki osobowe osoby fizycznej, natomiast przykładową konsekwencją takiego przetwarzania może być automatyczne odrzucenie elektronicznego wniosku kredytowego czy elektroniczne metody rekrutacji bez interwencji ludzkiej

WZÓR

ZAŁĄCZNIK NR 3 DO
POLITYKI BEZPIECZEŃSTWA

INFORMACJA O ZBIERANIU DANYCH OSOBOWYCH NIE OD OSOBY, KTÓREJ DOTYCZĄ

Na podstawie art. 14 ust. 1 i 2 rozporządzenia[76] ..... informuje, że:

1. Administratorem Pani/Pana* danych osobowych jest .....

   dane kontaktowe .....
2. Inspektorem ochrony danych jest ....., dane kontaktowe[77] .....
3. Pani/Pana* dane osobowe przetwarzane będą w celu[78] .....
   na podstawie[79] .....
4. Odbiorcą Pani/Pana* danych osobowych będą[80] .....
5. Pani/Pana* dane osobowe będą przechowywane przez okres[81] .....
6. Posiada Pani/Pan* prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania[82].
7. Ma Pani/Pana* prawo wniesienia skargi do PUODO gdy uzna Pani/Pan*, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy ogólnego Rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.
8. Podanie przez Panią/Pana* danych osobowych jest[83] .....

   Jest Pani/Pan* zobowiązana do ich podania, a konsekwencją niepodania danych osobowych będzie[84]:

   .....

   .....
9. Źródłem pochodzenia danych osobowych jest: .....
10. Pani/Pana* dane będą/ nie będą* podlegać zautomatyzowanemu podejmowaniu decyzji, w tym również profilowaniu. Zautomatyzowane podejmowanie decyzji będzie odbywało się na zasadach: .....

    .....

    konsekwencją takiego przetwarzania będzie[85]: .....

.....
Administrator Danych Osobowych

* niepotrzebne skreślić

[76] 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.

[77] e-mail lub inne dane kontaktowe.

[78] należy podać cel przetwarzania.

[79] należy podać podstawę prawną przetwarzania np. art. 6 ust 1 pkt a/b/c/d/e/f. *Przy podpunkcie f należy wskazać uzasadniony interes ADO lub strony trzeciej.

[80] można wymienić kategorię odbiorców o ile istnieją.

[81] jeżeli nie ma możliwości wskazania okresu przechowywania należy podać kryterium ustalania tego okresu np. do czasu wyłonienia zwycięzcy konkursu, do czasu zakończenia rekrutacji itd.

[82] jeżeli przetwarzanie odbywa się na podstawie zgody), którego dokonano na podstawie zgody przed jej cofnięciem.

[83] wybrać odpowiednio: wymogiem ustawowym/warunkiem umownym/warunkiem zawarcia umowy.

[84] jeżeli osoba, której dane dotyczą, jest zobowiązana do ich podania należy wskazać ewentualne konsekwencje niepodania danych.

[85] należy wskazać istotne informacje o zasadach zautomatyzowanego podejmowania decyzji oraz informacje o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą. Np. w jaki sposób będą oceniane czynniki osobowe osoby fizycznej, natomiast przykładową konsekwencją takiego przetwarzania może być automatyczne odrzucenie elektronicznego wniosku kredytowego czy elektroniczne metody rekrutacji bez interwencji ludzkiej

WZÓR

ZAŁĄCZNIK NR 4 DO
POLITYKI BEZPIECZEŃSTWA

INFORMACJA O PRZETWARZANIU DANYCH OSOBOWYCH

Na podstawie art. 15 ust. 1 i 3 rozporządzenia [86] .....
(nazwa administratora)

przekazuje następujące informacje:

1. Cele przetwarzania: .....

   .....

2. Kategorie odnośnych danych osobowych: .....

   .....

3. Informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych:

   .....

4. W miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu: .....

   .....

5. Informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania: .....

   .....

6. Informacje o prawie wniesienia skargi do organu nadzorczego: .....
7. Jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle: .....
8. Informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4[87], oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą: .....

.....
Administrator Danych Osobowych

* niepotrzebne skreślić

[86] 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.

[87] art. 22. 1 „Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.
2. Ust. 1 nie ma zastosowania, jeżeli ta decyzja:
a) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem;
b) jest dozwolona prawem Unii Europejskiej lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub
c) opiera się na wyraźnej zgodzie osoby, której dane dotyczą" RODO."

OCENA SKUTKÓW NARUSZENIA DANYCH

1.	**Kategorie danych**			
2.	**Kategorie osób, których dane dotyczą**			
3.	**Podstawa prawna przetwarzania danych**			
4.	**Okres retencji danych**			
5.	**Odbiorcy danych w państwach trzecich**			
6.	**Sposób zabezpieczenia przekazywania danych do państw trzecich**			
7.	**Odbiorcy danych**			
8.	**Czy osoba, której dane dotyczą ma możliwość realizacji praw, o których mowa w rozdz. III RODO**			
9.	**Czy realizowany jest obowiązek informacyjny, o którym mowa w art. 12, 13, 14 RODO**			
10.	**Opis planowanych operacji przetwarzania**			
11.	**Cel przetwarzania, w tym uzasadniony interes administratora danych**			
12.	**Ocena, czy operacje przetwarzania są niezbędne oraz proporcjonalne do celów**			
13.	**Ocena ryzyka naruszenia praw lub wolności osób, których dane dotyczą**			
14.	**Środki planowane w celu zaradzenia ryzyku**			

OCENA RYZYKA NARUSZENIA

1.	**Nazwa Administratora danych oraz dane kontaktowe**			
2.	**Dane kontaktowe Inspektora Ochrony Danych**			
3.	Nazwa czynności przetwarzania		Prawdopodobieństwo wystąpienia określonego zdarzenia będącego naruszeniem	Wielkość szkody, jakie zdarzenie to może spowodować w odniesieniu do osoby, której danę dotyczą
4.	Prawdopodobieństwo wystąpienia określonego zdarzenia będącego naruszeniem kształtuje się:			
5.	Czy dane osobowe są przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą[88];			
6.	Czy dane osobowe są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami[89];			
7.	Czy dane osobowe są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane[90];			
8.	Czy dane osobowe są prawidłowe i w razie potrzeby uaktualniane[91];			
9.	Czy dane osobowe są przechowywane w formie umożliwiającej identyfikację osoby, której dane			

[88] art. 5 ust. 1 lit. a RODO, („zgodność z prawem, rzetelność i przejrzystość").
[89] art. 5 ust. 1 lit. b RODO, [dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ograniczenie celu")].
[90] art. 5 ust. 1 lit. c RODO, („minimalizacja danych").
[91] art. 5 ust. 1 lit. d RODO, należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość").

	dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane[92];			
10.	Czy dane osobowe są przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych[93];			
11.	Czy do danych osobowych mają dostęp tylko osobowy upoważnione na podstawie wydanego upoważnienia przez organ[94].			

SZACOWANIE RYZYKA METODA ILOŚCIOWA:

prawdopodobieństwo wystąpienia określonego zdarzenia będącego naruszeniem:

$R_p = P \times (S_d + S_i + S_p)$

R_p – poziom wyliczenia ryzyka

P – wartość przypisana prawdopodobieństwu materializacji zagrożenia z zakresu (0,1,2,3,4),

gdzie:

0 – zdarzenie nieprawdopodobne,
1 – zdarzenie prawie, nieprawdopodobne,
2 – zdarzenie mało prawdopodobne,
3 – zdarzenie wysoce prawdopodobne,
4 – zdarzenie niemal pewne.

S_d, S_i, S_p – skutki zdarzenia odpowiednio w zakresie **dostępności** informacji, **integralności** oraz **poufności** z zakresu (0,1,2,3,4),

gdzie:

0 – zdarzenie nie powoduje skutku (nie występuje),
1 – zdarzenie wywołuje niewielki skutek,
2 – zdarzenie wywołuje znaczący skutek,
3 – zdarzenie wywołuje bardzo znaczący skutek,
4 – zdarzenie wywołuje skutek katastrofalny.

[92] art. 5 lit. e RODO, [dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania)"];
[93] art. 5 ust. 1 lit. f RODO, („integralność i poufność").
[94] art. 29 RODO.

WZÓR

ZAŁĄCZNIK NR 7 DO
POLITYKI BEZPIECZEŃSTWA

LISTA OSÓB UCZESTNIKÓW SZKOLENIA Z ZAKRESU OCHRONY DANYCH OSOBOWYCH

Lp.	Imię i nazwisko pracownika	Data	Podpis pracownika
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			

.....
(podpis prowadzącego szkolenie)

WZÓR

ZAŁĄCZNIK NR 8 DO
POLITYKI BEZPIECZEŃSTWA

ANKIETA
SPRAWDZENIE WIEDZY PRACOWNIKÓW Z ZAKRESU OCHRONY DANYCH

Ankieta jest w pełni anonimowa. Wyniki nie będą udostępniane Twojemu przełożonemu. Wyniki ankiety służą wyłącznie zebraniu statystycznych informacji na temat poziomu wiedzy z zakresu ochrony danych osobowych wśród pracowników.

Prosi się o samodzielne rozwiązanie ankiety i udzielanie szczerych odpowiedzi. Tylko wtedy wyniki będą wartościowe. Jeśli nie znasz odpowiedzi, wpisz "nie wiem".

Jak często zmieniasz hasła dostępu do systemów informatycznych w których przetwarzane są dane osobowe?	☐ w ogóle nie zmieniam; ☐ zmieniam nieregularnie; ☐ zmieniam regularnie co 30 dni; ☐ zmieniam rzadziej niż co 45 dni;
W celu weryfikacji odpowiedniej składni hasła – wpisz hasło, którym logujesz się do dowolnie wybranego przez siebie systemu informatycznego	.....
Wpisz imię i nazwisko osoby pełniącej funkcję Inspektora Ochrony Danych	.....
W jaki sposób blokujesz komputer jeśli odchodzisz na przerwę?	.....
Wśród wskazanych zestawów informacji wskaż te, które stanowią dane osobowe	☐ służbowy adres e-mail; ☐ PESEL: 80203410235; ☐ Jan Kowalski; ☐ Mat-kot Marek Kot, NIP: 522-23-34-566;
Do jakich danych masz dostęp wg nadanego Ci upoważnienia do przetwarzania danych osobowych?	.....
Jeśli w drugim pytaniu ujawniłeś swoje hasło, prosimy o jego zamazanie	.....
Wskaż czynności, które są przetwarzaniem danych osobowych	☐ przechowywanie wydruków z danymi w szufladzie; ☐ kopiowanie baz danych na pendrive; ☐ edytowanie pliku Excel z danymi osobowymi; ☐ przeglądanie skrzynki mailowej;

WZÓR

ZAŁĄCZNIK NR 9 DO
POLITYKI BEZPIECZEŃSTWA

RAPORT
ZE SPRAWDZANIA ZGODNOŚCI I PRZETWARZANIA DANYCH OSOBOWYCH Z PRZEPISAMI O OCHRONIE DANYCH OSOBOWYCH

1. Oznaczenie administratora danych i adres jego siedziby:

.....

(podać pełną nazwę oraz adres)

2. Imię i nazwisko Inspektora Ochrony Danych:

.....

3. Wykaz czynności podjętych przez inspektora ochrony danych w toku sprawdzenia oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach:

.....

4. Datę rozpoczęcia i zakończenia sprawdzenia:

.....

5. Określenie przedmiotu i zakresu sprawdzenia:

.....

6. Opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych:

.....

7. Stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem:

.....

8. Wyszczególnienie załączników stanowiących składową część sprawozdania:

.....

……

Data, miejsce i podpis Inspektora Ochrony Danych

WZÓR

ZAŁĄCZNIK NR 10 DO
POLITYKI BEZPIECZEŃSTWA

INWENTARYZACJA ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

Lp.	Nazwa zbioru	Programy służące do przetwarzania danych	Lokalizacja zbioru/zasobu	Miejsce przetwarzania danych
1	2	3	4	6
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				
21.				
22.				

REJESTR UMÓW
POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Nazwa podmiotu, któremu powierzono dane	Data powierzenia	Cel powierzenia/ numer umowy powierzenia	Zakres powierzonych danych *(jakie dane zostały powierzone)*	Określenie zbioru/zasobu
1	2	3	4	5	6
1.					
2.					
3.					
4.					
5.					
6.					
7.					

UMOWA
POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w dniu ..... w ..... pomiędzy:

.....

reprezentowanym przez: .....

zwanym dalej „**Administratorem**”;

a

.....

reprezentowaną przez: .....

zwanym dalej „**Przetwarzającym**”;

zwanymi dalej Stronami

§ 1.
PRZEDMIOT UMOWY

1. Strony zawarły Umowę podstawową z dnia ..... r. w związku, z wykonywaniem której Administrator powierzył Przetwarzającemu przetwarzanie danych osobowych w zakresie określonym Umową;
2. Celem Umowy jest ustalenie warunków, na jakich Przetwarzający wykonuje operacje przetwarzania Danych Osobowych w imieniu Administratora;
3. Strony zawierając Umowę dążą do takiego uregulowania zasad przetwarzania Danych Osobowych, aby odpowiadały one w pełni postanowieniom 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) – dalej RODO.
4. Strony postanowiły zawrzeć Umowę o następującej treści:
   1) przedmiot i czas trwania przetwarzania;
   2) charakter i cel przetwarzania;
   3) rodzaj danych osobowych oraz kategorie osób, których dane dotyczą;
   4) obowiązki i prawa administratora.

§ 2.
OPIS PRZETWARZANIA[95]

1. Na warunkach określonych niniejszą Umową oraz Umową Podstawową Administrator powierza Przetwarzającemu przetwarzanie (w rozumieniu RODO) dalej opisanych Danych Osobowych.
   1) Przetwarzanie będzie wykonywane w okresie obowiązywania Umowy Podstawowej.
   2) Charakter i cel przetwarzania wynikają z Umowy Podstawowej.
   3) Przetwarzanie obejmować będzie następujące rodzaje danych osobowych („**Dane**”):

[95] art. 28 ust. 3 RODO

a) Dane zwykłe:

a. .....

b. .....

c. .....

b) Dane wrażliwe:

a. .....

b. .....

c. .....

4) Przetwarzanie Danych będzie dotyczyć następujących kategorii osób:

a) pracownicy Administratora i podmiotów stowarzyszonych Administratora;

b) klienci usługi/produktu Administratora określonych w Umowie Podstawowej;

c) osoby, z którymi klienci Administratora wchodzą w interakcje społeczne;

d) kontrahenci (odbiorcy i dostawcy) klientów administratora;

e) odbiorcy korespondencji elektronicznej klientów Administratora.

2. Podpowierzenie[96]

1) Przetwarzający może powierzyć konkretne operacje przetwarzania Danych („podpowierzenie") w drodze pisemnej umowy podpowierzenia („Umowa Podpowierzenia") innym podmiotom przetwarzającym („Podprzetwarzający"), pod warunkiem uprzedniej akceptacji Podprzetwarzającego przez Administratora lub braku sprzeciwu.

2) Powierzenie przetwarzania Danych Podprzetwarzającym wymaga uprzedniego zgłoszenia Administratorowi w celu umożliwienia wyrażenia sprzeciwu. Administrator może z uzasadnionych przyczyn zgłosić udokumentowany sprzeciw względem powierzenia Danych konkretnemu Podprzetwarzającemu. W razie zgłoszenia sprzeciwu Przetwarzający nie ma prawa powierzyć Danych Podprzetwarzającemu objętemu sprzeciwem, a jeżeli sprzeciw dotyczy aktualnego Podprzetwarzającego, musi niezwłocznie zakończyć podpowierzenie temu Podprzetwarzającemu. Wątpliwości co do zasadności sprzeciwu i ewentualnych negatywnych konsekwencji Przetwarzający zgłosi Administratorowi w czasie umożliwiającym zapewnienie ciągłości przetwarzania.

3) Dokonując podpowierzenia[97] Przetwarzający ma obowiązek zobowiązać Podprzetwarzającego do realizacji wszystkich obowiązków Przetwarzającego wynikających z niniejszej Umowy powierzenia, z wyjątkiem tych, które nie mają zastosowania ze względu na naturę konkretnego podpowierzenia.

4) Przetwarzający ma obowiązek zapewnić, aby Podprzetwarzający złożył Administratorowi zobowiązanie do wykonania obowiązków, o których mowa w poprzednim ustępie. Może to zostać wykonane przez podpisanie stosownego oświadczenia adresowanego do Administratora wraz z podpisaniem Umowy Podpowierzenia, zawierającego listę obowiązków Podprzetwarzającego.

5) Przetwarzający nie ma prawa przekazać Podprzetwarzającemu całości wykonania Umowy.

[96] art. 28 ust. 2 RODO

[97] art. 28 ust. 4 RODO

§ 3.
OBOWIĄZKI PRZETWARZAJĄCEGO

Przetwarzający ma następujące obowiązki:

1) przetwarzający przetwarza Dane wyłącznie zgodnie z udokumentowanymi poleceniami lub instrukcjami Administratora.

2) przetwarzający oświadcza, że nie przekazuje Danych do państwa trzeciego lub organizacji międzynarodowej[98] (czyli poza Europejski Obszar Gospodarczy („EOG")). Przetwarzający oświadcza również, że nie korzysta z podwykonawców, którzy przekazują Dane poza EOG.

3) jeżeli Przetwarzający ma zamiar lub obowiązek przekazywać Dane poza EOG, informuje o tym Administratora, w celu umożliwienia Administratorowi podjęcia decyzji i działań niezbędnych do zapewnienia zgodności przetwarzania z prawem lub zakończenia powierzenia przetwarzania.

4) przetwarzający uzyskuje od osób, które zostały upoważnione do przetwarzania Danych w wykonaniu Umowy[99], udokumentowane zobowiązania do zachowania tajemnicy, ewentualnie upewnia się, że te osoby podlegają ustawowemu obowiązkowi zachowania tajemnicy.

5) przetwarzający zapewnia ochronę Danych[100] i podejmuje środki ochrony danych, o których mowa w art. 32 RODO, zgodnie z dalszymi postanowieniami Umowy.

6) przetwarzający przestrzega warunków korzystania z usług innego podmiotu przetwarzającego[101] (Podprzetwarzającego).

7) przetwarzający zobowiązuje się wobec Administratora do odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania praw określonych w rozdziale III RODO („Prawa jednostki")[102]. Przetwarzający oświadcza, że zapewnia obsługę Praw jednostki w odniesieniu do powierzonych Danych. Szczegóły obsługi Praw jednostki zostaną pomiędzy Stronami uzgodnione. Strony ustaliły procedurę obsługi Praw jednostki odrębnym dokumentem.

8) przetwarzający współpracuje z Administratorem[103] przy wykonywaniu przez Administratora obowiązków z obszaru ochrony danych osobowych, o których mowa w art. 32−36 RODO (ochrona danych, zgłaszanie naruszeń organowi nadzorczemu, zawiadamianie osób dotkniętych naruszeniem ochrony danych, ocena skutków dla ochrony danych i uprzednie konsultacje z organem nadzorczym).

9) jeżeli Przetwarzający poweźmie wątpliwości co do zgodności z prawem wydanych przez Administratora poleceń lub instrukcji, Przetwarzający natychmiast informuje Administratora o stwierdzonej wątpliwości[104] (w sposób udokumentowany i z uzasadnieniem), pod rygorem utraty możliwości dochodzenia roszczeń przeciwko Administratorowi z tego tytułu.

10) planując dokonanie zmian w sposobie przetwarzania Danych[105], Przetwarzający ma obowiązek zastosować się do wymogu projektowania prywatności, o którym mowa w art. 25 ust. 1 RODO i ma obowiązek z wyprzedzeniem informować Administratora o planowanych zmianach w taki sposób i terminach, aby zapewnić Administratorowi realną możliwość reagowania, jeżeli planowane

[98] art. 28 ust. 3 lit. a RODO
[99] art. 28 ust. 3 lit. b RODO
[100] art. 28 ust. 3 lit. c RODO
[101] art. 28 ust. 3 lit. d RODO.
[102] art. 28 ust. 3 lit. e RODO.
[103] art. 28 ust. 3 lit. f RODO
[104] art. 28 ust. 3 ak. 2 RODO.
[105] art. 25 ust. 1 RODO.

przez Przetwarzającego zmiany w opinii Administratora grożą uzgodnionemu poziomowi bezpieczeństwa Danych lub zwiększają ryzyko naruszenia praw lub wolności osób, wskutek przetwarzania Danych przez Przetwarzającego.

11) przetwarzający zobowiązuje się do ograniczenia dostępu do Danych Osobowych wyłącznie do osób, których dostęp do Danych[106] jest potrzebny dla realizacji Umowy i posiadających odpowiednie upoważnienie.

12) przetwarzający zobowiązuje się do prowadzenia dokumentacji opisującej sposób przetwarzania Danych, w tym rejestru czynności przetwarzania danych osobowych[107]. Przetwarzający udostępniania na żądanie Administratora prowadzony rejestr czynności przetwarzania danych przetwarzającego, z wyłączeniem informacji stanowiących tajemnicę handlową innych klientów Przetwarzającego.

13) jeżeli Przetwarzający wykorzystuje w celu realizacji Umowy zautomatyzowane przetwarzanie[108], w tym profilowanie, o którym mowa w art. 22 ust. 1 i 4 RODO, Przetwarzający informuje o tym Administratora w celu i w zakresie niezbędnym do wykonania przez Administratora obowiązku informacyjnego.

14) przetwarzający ma obowiązek zapewnić osobom upoważnionym do przetwarzania Danych odpowiednie szkolenie z zakresu ochrony danych osobowych.

§ 4.
OBOWIĄZKI ADMINISTRATORA

Administrator zobowiązany jest współdziałać z Przetwarzającym w wykonaniu Umowy, udzielać Przetwarzającemu wyjaśnień w razie wątpliwości co do legalności poleceń Administratora, jak też wywiązywać się terminowo ze swoich szczegółowych obowiązków.

§ 5.
BEZPIECZEŃSTWO DANYCH OSOBOWYCH

1. Bezpieczeństwo danych osobowych [art. 32 RODO] – przetwarzający przeprowadził analizę ryzyka przetwarzania powierzonych Danych, udostępnił ją Administratorowi i stosuje się do jej wyników, co do organizacyjnych i technicznych środków ochrony danych.
2. Środki bezpieczeństwa – strony uzgodniły odrębnym dokumentem poziom zabezpieczeń Danych wymagany po stronie Przetwarzającego.
3. Gwarancje bezpieczeństwa – przetwarzający przedstawił Administratorowi informacje i dokumenty potwierdzające, że Przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych. Obie Strony zachowują kopie przedstawionych dokumentów i dowody przedstawienia informacji, dla potrzeb spełnienia wymogu rozliczalności.

[106] art. 25 ust. 2 RODO.
[107] art. 30 ust. 2RODO.
[108] art. 13 i 14 RODO.

§ 6.
POWIADOMIENIE O NARUSZENIACH DANYCH OSOBOWYCH

1. Powiadomienie o naruszeniu – Przetwarzający powiadamia Administratora danych o każdym podejrzeniu naruszenia ochrony Danych osobowych nie później niż w 24 godziny od pierwszego zgłoszenia, umożliwia Administratorowi uczestnictwo w czynnościach wyjaśniających i informuje Administratora o ustaleniach z chwilą ich dokonania, w szczególności o stwierdzeniu naruszenia.
2. Rozwinięcie – powiadomienie o stwierdzeniu naruszenia, powinno być przesłane wraz z wszelką niezbędną dokumentacją dotyczącą naruszenia, aby umożliwić Administratorowi spełnienie obowiązku powiadomienia organ nadzoru.
3. Nadzór:
    1) Sprawowanie kontroli [art. 28 ust. 3 lit. h RODO] – Administrator kontroluje sposób przetwarzania powierzonych Danych Osobowych po uprzednim poinformowaniu Przetwarzającego o planowanej kontroli. Administrator lub wyznaczone przez niego osoby są uprawnione do wstępu do pomieszczeń, w których przetwarzane są Dane Osobowe oraz wglądu do dokumentacji związanej z przetwarzaniem Danych Osobowych. Administrator uprawniony jest do żądania od Przetwarzającego udzielania informacji dotyczących przebiegu przetwarzania Danych Osobowych, oraz udostępnienia rejestrów przetwarzania.
    2) Współpraca przy kontroli [art. 28 ust. 3 lit. h RODO] – Przetwarzający współpracuje z Urzędem Ochrony Danych Osobowych w zakresie wykonywanych przez niego zadań.
    3) Przetwarzający:
        a) udostępnia Administratorowi wszelkie informacje niezbędne do wykazania zgodności działania Administratora z przepisami RODO;
        b) umożliwia Administratorowi lub upoważnionemu audytorowi przeprowadzanie audytów lub inspekcji. Przetwarzający współpracuje w zakresie realizacji audytów lub inspekcji.

§ 7.
OŚWIADCZENIA STRON

1. Oświadczenie Administratora: Administrator oświadcza, że jest Administratorem Danych Osobowych oraz, że jest uprawniony do ich przetwarzania w zakresie, w jakim powierzył je Przetwarzającemu.
2. Oświadczenie Przetwarzającego [art. 28 ust. 1 RODO]: Przetwarzający oświadcza, że w ramach prowadzonej działalności gospodarczej profesjonalnie zajmuje się przetwarzaniem danych osobowych objętym Umowa i Umową Podstawową, posiada w tym zakresie niezbędną wiedzę, odpowiednie środki techniczne i organizacyjne oraz daje rękojmię należytego wykonania niniejszej Umowy.
3. Referencje [art. 28 ust. 1 RODO]: na żądanie Administratora Przetwarzający okaże stosowne referencje, wykaz doświadczenia, informacje finansowe lub inne dowody, iż Przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

§ 8.
ODPOWIEDZIALNOŚĆ

1. Odpowiedzialność Przetwarzającego [art. 82 ust. 3 RODO]: Przetwarzający odpowiada za szkody spowodowane swoim działaniem w związku z niedopełnieniem obowiązków, które RODO nakłada bezpośrednio na Przetwarzającego lub gdy działał poza zgodnymi z prawem instrukcjami Administratora

lub wbrew tym instrukcjom. Przetwarzający odpowiada za szkody spowodowane zastosowaniem lub nie zastosowaniem właściwych środków bezpieczeństwa.

2. Odpowiedzialność za Podprzetwarzających [art. 28 ust. 4 RODO]: jeżeli Podprzetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków przez Podprzetwarzającego spoczywa na Przetwarzającym.

§ 9.
OKRES OBOWIĄZYWANIA UMOWY POWIERZENIA [ART. 28 UST. 3 RODO]

Umowa została zawarta na czas obowiązywania Umowy Podstawowej.

§ 10.
USUNIĘCIE DANYCH

1. Usunięcie danych [art. 28 ust. 3 lit g RODO]: z chwilą rozwiązania Umowy: Przetwarzający nie ma prawa do dalszego przetwarzania powierzonych Danych i jest zobowiązany do:
   1) usunięcia powierzonych danych;
   2) usunięcia wszelkich ich istniejących kopii lub zwrotu Danych, chyba że Administrator postanowi inaczej lub prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują dalej przechowywanie Danych.
2. Strony uzgodnią sposób usunięcia Danych odrębnym dokumentem w ciągu 30 dni od zawarcia Umowy Powierzenia.
3. Przetwarzający dokona usunięcia Danych po upływie 180 dni od zakończenia Umowy, chyba że Administrator poleci mu to uczynić wcześniej.
4. Po wykonaniu zobowiązania, o którym mowa w pkt ust. 1 i 3, Przetwarzający złoży Administratorowi pisemne oświadczenie potwierdzające trwałe usunięcie wszystkich Danych.

§ 11.
POSTANOWIENIA KOŃCOWE

1. W razie sprzeczności pomiędzy postanowieniami niniejszej Umowy Powierzenia a Umowy Podstawowej, pierwszeństwo mają postanowienia Umowy Powierzenia. Oznacza to także, że kwestie dotyczące przetwarzania danych osobowych pomiędzy Administratorem a Przetwarzającym należy regulować poprzez zmiany niniejszej Umowy lub w wykonaniu jej postanowień.
2. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
3. Umowa podlega prawu polskiemu oraz RODO.

.....
Administrator Przetwarzający

UMOWA
O WSPÓŁADMINISTROWANIE DANYMI OSOBOWYMI

Niniejsza umowa o współadministrowanie danymi osobowymi z dnia ..... roku zostawała zawarta w .....,

POMIĘDZY:

.....

reprezentowaną przez: .....

zwanym dalej „**Administratorem 1**";

a

.....

reprezentowaną przez: .....

zwanym dalej „**Administratorem 2**";

(zwanymi dalej łącznie: „**Współadministratorami**" lub „**Stronami**" bądź każda z osobna „**Współadministratorem**" lub „**Stroną**").

§ 1.
POSTANOWIENIA ogólne

1. Definicje

1) „Administrator 1"	.....
2) „Administrator 2"	.....
3) „Dane Osobowe"	dane osobowe w rozumieniu RODO, w tym Dane Wrażliwe.
4) „Dane Wrażliwe"	szczególne kategorie danych osobowych wymienione w art. 9 ust. 1 RODO.
5) „Dzień Roboczy"	dowolny dzień, za wyjątkiem sobót, niedziel lub innych dni, które są dniami częściowo lub całkowicie wolnymi od pracy w Polsce w rozumieniu ustawy z dnia 18.01.1951 r. o dniach wolnych od pracy (tj. Dz. U. z 2015 r., poz. 90).
6) „Przetwarzanie"	operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczenie, usuwanie lub niszczenie oraz inne formy przetwarzania w rozumieniu RODO.

7)	**„Podmiot Przetwarzający”**	osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który Przetwarza Dane Osobowe w imieniu Administratora.
8)	**„RODO”**	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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).
9)	**„Umowa”**	niniejszą umowę o współadministrowanie przetwarzaniem Danych Osobowych zawartą w dniu ..... w ....., pomiędzy Współadministratorami.
10)	**„Umowa Podstawowa”**	oznacza umowę zawartą w dniu ..... w ....., w związku z wykonywaniem której Współadministratorzy uzyskali uprawnienia do ustalania łącznie celów i sposobów Przetwarzania Danych Osobowych.
11)	**„Współprzetwarzanie”**	oznacza Przetwarzanie, w którym co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania.

§ 2.
OŚWIADCZENIA STRON

1. Współadministratorzy oświadczają i zapewniają, iż są uprawnieni do ustalania łącznie z drugim Współadministratorem celów i sposobów Przetwarzania Danych Osobowych.
2. Współadministratorzy oświadczają, że znane im są zasady przetwarzania i zabezpieczenia Danych Osobowych wynikające z RODO oraz innych przepisów prawa powszechnie obowiązującego, ze szczególnym uwzględnieniem obowiązków administratora Danych Osobowych.
3. Współadministratorzy oświadczają i zapewniają, iż zgodnie z art. 24 RODO posiadają środki techniczne i organizacyjne, mające na celu zapewnienie zgodności przetwarzania Danych Osobowych z przepisami RODO oraz stosują środki bezpieczeństwa spełniające wymogi RODO, a także poddają je przeglądom i uaktualnieniom.
4. Każda Strona oświadcza i zapewnia, że została prawidłowo ustanowiona i istnieje zgodnie z obowiązującymi przepisami prawa i posiada wszelkie wymagane uprawnienia prawne i korporacyjne oraz prawo do zawarcia Umowy i wykonywania swoich zobowiązań z niej wynikających, a niniejsza Umowa stanowi ważne i wiążące zobowiązanie podlegające wykonaniu przez Strony.

§ 3.
PRZEDMIOT umowy

1. Niniejsza Umowa reguluje wzajemne stosunki pomiędzy Stronami w zakresie Współadministrowania Danymi Osobowymi, a w szczególności ustala w przejrzysty sposób zakresy odpowiedzialności Współadministratorów dotyczące wypełniania obowiązków wynikających z przepisów RODO i innych

przepisów prawa powszechnie obowiązującego, jak również określa reprezentację Współadministratorów,

w stosunku do podmiotów, których Dane Osobowe dotyczą oraz ich relacje z tymi podmiotami.

2. Dla potrzeb prawidłowej realizacji niniejszej Umowy Współadministratorzy zobowiązują się:
   1) współpracować przy realizacji obowiązków ciążących na Współadministratorach Danych Osobowych;
   2) przetwarzać powierzone im Dane Osobowe zgodnie z niniejszą Umową, Umową Podstawową, przepisami RODO oraz innymi przepisami prawa powszechnie obowiązującego;
   3) powstrzymywać się od działań faktycznych i prawnych, które mogłyby w jakikolwiek sposób naruszyć bezpieczeństwo Danych Osobowych albo narazić drugiego Współadministratora na odpowiedzialność cywilną, administracyjną lub karną.
3. W celu uniknięcia wątpliwości, z tytułu realizacji obowiązków wynikających z niniejszej Umowy, żadnemu ze Współadministratorów nie przysługuje wynagrodzenie ani prawo do żądania podwyższenia wynagrodzenia należnego Współadministratorowi, wynikającego z Umowy Podstawowej albo z innego stosunku prawnego.
4. Każdy Współadministrator pokrywa własne koszty i wydatki związane z prawidłowym wykonaniem niniejszej Umowy.

§ 4.
Czas TRWANIA Umowy

1. Niniejsza Umowa została zawarta na czas określony, na okres, przez który, na podstawie Umowy Podstawowej, Współadministratorzy wspólnie ustalają cele i sposoby Przetwarzania Danych Osobowych.
2. W przypadku każdej zmiany układu Administratorów (Współadministratorów) Danych Osobowych przetwarzanych na podstawie Umowy Podstawowej, Strony, negocjując w dobrej wierze warunki zmiany niniejszej Umowy, zawrą aneks do Umowy, na podstawie którego wszyscy Administratorzy (Współadministratorzy) Danych Osobowych przystąpią do Umowy na prawach Strony.

§ 5.
OBOWIĄZKI Stron

1. Współadministratorzy zobowiązani są zapewnić bezpieczeństwo przetwarzania Danych Osobowych poprzez wdrożenie odpowiednich środków technicznych i organizacyjnych, adekwatnych do rodzaju Danych Osobowych oraz ryzyka naruszenia praw osób, których te dane dotyczą.
2. Współadministratorzy ustalają, że w zakresie udzielania odpowiedzi na żądania osoby, której dane dotyczą, (w szczególności dotyczy to żądań i oświadczeń w zakresie prawa do informowania i przejrzystej komunikacji, dostępu do Danych Osobowych, sprostowania, usunięcia, ograniczenia przetwarzania, przenoszenia Danych Osobowych, sprzeciwu wobec przetwarzania Danych Osobowych)

właściwy będzie Współadministrator, który otrzymał dane żądanie lub oświadczenie. W przypadku, gdy żądanie zostanie skierowane do obydwu Współadministratorów, to obydwaj Współadministratorzy zobowiązani będą, każdy z osobna, do udzielenia ww. odpowiedzi, po wcześniejszym uzgodnieniu wspólnego stanowiska. Niezależnie od powyższego, Współadministratorzy są zobowiązani współpracować między sobą w zakresie udzielania odpowiedzi na żądania osoby, której dane dotyczą. W tym celu Współadministrator zobowiązany jest niezwłocznie poinformować drugiego Współadministratora o każdym żądaniu osoby uprawnionej w ramach wykonywania przez tę osobę praw wynikających z RODO oraz udzielać drugiemu Współadministratorowi wszelkich niezbędnych informacji w tym zakresie.

3. Współadministratorzy ustalają, że w zakresie wywiązywania się przez Współadministratorów z obowiązków w zakresie zarządzania naruszeniami ochrony Danych Osobowych oraz ich zgłaszania do organu nadzoru oraz osoby, której dane dotyczą, właściwy będzie Współadministrator, który stwierdził naruszenie. W przypadku, gdy naruszenie zostanie stwierdzone przez obydwu Współadministratorów (np. gdy zostało zgłoszone obydwu Współadministratorom), to właściwy do wykonania obowiązków określonych w art. 33 - 34 RODO będzie ten Współadministrator, z którego działania bądź zaniechania naruszenie wynikło. Niezależnie od powyższego, Współadministratorzy są zobowiązani współpracować między sobąw zakresie spełniania obowiązków określonych w art. 33 - 34 RODO. W tym celu Współadministrator zobowiązany jest niezwłocznie poinformować drugiego Współadministratora o każdym stwierdzonym naruszeniu ochrony Danych Osobowych, podjętych w związku z naruszeniem krokach, treści zgłoszenia przekazanego organowi nadzorczemu w związku z naruszeniem oraz udzielić drugiemu Współadministratorowi wszelkich niezbędnych informacji w tym zakresie.
4. W przypadku, gdy dany rodzaj Przetwarzania stosowany przez Współadministratora – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Współadministrator przed rozpoczęciem Przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych i jest zobowiązany do spełnienia obowiązków określonych w art. 35 – 36 RODO. Współadministrator, o którym mowa w zdaniu poprzedzającym, zobowiązany jest niezwłocznie poinformować drugiego Współadministratora o stwierdzeniu konieczności dokonania oceny skutków dla ochrony Danych Osobowych oraz przeprowadzenia konsultacji z organem nadzoru oraz udzielać drugiemu Współadministratorowi wszelkich niezbędnych informacji w tym zakresie.
5. Każdy Współadministrator jest zobowiązany we własnym zakresie prowadzić rejestr czynności przetwarzania, o którym mowa w art. 30 RODO.
6. Wszelka korespondencja pomiędzy Współadministratorami powinna być przesyłana w sposób zapewniający bezpieczeństwo przekazywanych informacji, tj. w formie zaszyfrowanej.

§ 6.
ZAPEWNIENIE BEZPIECZEŃSTWA Danych Osobowych

1. Dostęp do Danych Osobowych mogą mieć jedynie pracownicy lub współpracownicy Współadministratora, którzy otrzymali jego upoważnienie do przetwarzania tych danych, poprzedzone złożeniem przez te osoby oświadczenia o zachowaniu tych danych oraz sposobie ich zabezpieczenia w tajemnicy.
2. Współadministratorzy zobowiązani są wdrożyć dokumentację i procesy zapewniające sposób ochrony Danych Osobowych określony w RODO, w szczególności:
   1) własną dokumentację ochrony Danych Osobowych, uwzględniając charakter, zakres, kontekst i cele przetwarzania Danych Osobowych oraz ryzyko naruszenia praw lub wolności osób fizycznych;
   2) procedurę zapewniania osobom, których Dane Osobowe dotyczą, prawa dostępu do danych oraz związaną z tym procedurę wymiany informacji z drugim Współadministratorem;
   3) procedurę usuwania danych nadmiarowych, w związku z prawem osób, których Dane Osobowe dotyczą, „do bycia zapomnianym";
   4) procedurę obsługi naruszeń ochrony Danych Osobowych wraz z procedurą informowania drugiego Współadministratora;
   5) procedurę ograniczenia przetwarzania Danych Osobowych w sytuacjach wskazanych w RODO.

§ 7.
POWIERZANIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Współadministratorzy mogą zlecać Podmiotom Przetwarzającym realizację określonych czynności w zakresie przetwarzania Danych Osobowych. Podmioty Przetwarzające mogą przetwarzać Dane Osobowe wyłącznie w celu realizacji czynności, w odniesieniu, do których Dane Osobowe zostały przekazane Współadministratorom, i nie mogą przetwarzać Danych Osobowych w żadnych innych celach. W przypadku zlecenia czynności Podmiotowi Przetwarzającemu przez Współadministratora, Podmiot Przetwarzający będzie podlegać pisemnym zobowiązaniom w zakresie ochrony Danych Osobowych określonym w art. 28 RODO, zapewniając co najmniej taki sam poziom ochrony, jak określono w niniejszej Umowie.
2. W przypadku niewykonania przez Podmiot Przetwarzający ciążących na nim obowiązków w zakresie ochrony Danych Osobowych, Współadministrator, który powierzył Podmiotowi Przetwarzającemu Przetwarzanie Danych Osobowych – zgodnie z postanowieniami dotyczącymi odpowiedzialności w Umowie – ponosi pełną odpowiedzialność wobec drugiego Współadministratora za wykonanie zobowiązań ciążących na Podmiocie Przetwarzającym.
3. Zabronione jest umożliwienie dostępu do Danych Osobowych podmiotom, z którymi nie została zawarta umowa powierzenia przetwarzania Danych Osobowych (za wyjątkiem podmiotów Przetwarzających Dane Osobowe z upoważnienia Administratora lub Przetwarzającego).

4. Zabronione jest powierzenie Danych Osobowych przez Współadministratora Podmiotowi Przetwarzającemu z państwa trzeciego (tj. spoza UE/EOG, z wyłączeniem Szwajcarii) bez wcześniejszej pisemnej zgody drugiego Współadministratora. W przypadku zlecenia przez Współadministratora czynności Podmiotowi Przetwarzającemu z państwa trzeciego (tj. spoza UE/EOG, z wyłączeniem Szwajcarii), Współadministrator stosuje mechanizmy przesyłania danych zgodnie z art. 44 i następnymi RODO.

   W szczególności Współadministrator w wystarczający sposób zabezpiecza wdrożenie odpowiednich środków technicznych i organizacyjnych w taki sposób, aby przetwarzanie danych spełniało wymagania RODO, zapewnia ochronę praw zainteresowanych osób, których dane dotyczą, prowadzi rejestr transferów danych i dokumentację stosownych zabezpieczeń.

§ 8.
PRAWO KONTROLI

1. Współadministratorzy zobowiązani są udzielać sobie nawzajem wszelkich informacji niezbędnych dla wykazania wywiązywania się ze wszystkich obowiązków określonych w RODO.
2. Każdy Współadministrator zobowiązany jest, bez zbędnej zwłoki, powiadomić drugiego Współadministratora o wszelkich skargach, pismach, kontrolach organu nadzoru, postępowaniach sądowych i administracyjnych pozostających w związku z powierzonymi Danymi Osobowymi oraz udostępniać Współadministratorowi wszelką dokumentację z tym związaną.

§ 9.
ODPOWIEDZIALNOŚĆ

1. Każdy Współadministrator odpowiada za działania i zaniechania osób, przy pomocy których będzie przetwarzał powierzone Dane Osobowe (w tym Podmiotów Przetwarzających), jak za działania lub zaniechania własne.
2. Każdy Współadministrator odpowiada za szkody spowodowane swoim działaniem w związku z niedopełnieniem obowiązków, które RODO nakłada bezpośrednio na Administratora.
3. Każdy Współadministrator odpowiada za szkody spowodowane niezastosowaniem właściwych środków bezpieczeństwa.
4. Współadministrator dopuszczający się naruszenia przepisów RODO lub innych przepisów prawa powszechnie obowiązującego jest zobowiązany, w ramach swojej odpowiedzialności za przetwarzanie Danych Osobowych, do współpracy z drugim Współadministratorem w razie postępowania przed organem nadzorczym lub sporu sądowego z podmiotem Danych Osobowych.
5. W przypadku, gdy Podmiot Przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony Danych Osobowych, pełna odpowiedzialność za wypełnienie obowiązków przez Podmiot Przetwarzający spoczywa na Współadministratorze, który powierzył mu Przetwarzanie.

§ 10.
ZASADY ZACHOWANIA POUFNOŚCI

1. Współadministratorzy gwarantują, że osoby upoważnione do przetwarzania Danych Osobowych będą zobowiązane do zachowania tajemnicy na podstawie umowy lub będą podlegały podobnemu obowiązkowi wynikającemu z mocy prawa.
2. Z zastrzeżeniem postanowień Umowy, Umowy Podstawowej i przepisów prawa powszechnie obowiązującego, Strony mają obowiązek ochrony informacji poufnych, niezależnie od formy ich przekazania i przetwarzania (dalej: „**Informacje poufne**"), takich jak:
   1) Dane Osobowe, w tym w szczególności Dane Wrażliwe;
   2) informacje stanowiące tajemnicę przedsiębiorstwa (w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji);
   3) informacje wymagające ochrony bez względu na fakt, czy są one utrwalone w formie pisemnej lub w jakikolwiek inny sposób, zapisane w jakiejkolwiek formie i na jakimkolwiek nośniku, dotyczące Współadministratora lub jego klientów, kontrahentów, dostawców, a także informacje dotyczące usług, polityki cenowej, sprzedaży, wynagrodzeń pracowników, które Współadministrator otrzymał w okresie obowiązywania Umowy, Umowy Podstawowej lub o których dowiedział się, czy też do których miał dostęp lub będzie w ich posiadaniu w związku z prowadzonymi rozmowami i negocjacjami, a które nie są powszechnie znane.
3. Strony w szczególności zapewniają, że:
   1) wszelkie przekazane, udostępnione lub ujawnione przez drugą Stronę Informacje poufne będą chronione i zachowane w tajemnicy, w sposób zgodny z obowiązującymi przepisami prawa oraz postanowieniami Umowy oraz Umowy Podstawowej;
   2) uzyskane Informacje poufne zostaną użyte i wykorzystane wyłącznie w celu, w jakim zostały przekazane, udostępnione lub ujawnione;
   3) posiadane Informacje poufne nie zostaną przekazane ani ujawnione żadnej osobie trzeciej – bezpośrednio ani pośrednio (z zastrzeżeniem wyjątków przewidzianych w Umowie lub Umowie Podstawowej) – bez uprzedniej zgody drugiej Strony, wyrażonej w formie pisemnej;
   4) będą chronić na swój koszt Informacje poufne poprzez dołożenie najwyższego poziomu staranności przy zapewnieniu odpowiedniej infrastruktury zabezpieczającej przed ich nieuprawnionym ujawnieniem.
4. Strony będą zwolnione z obowiązku zachowania w tajemnicy Informacji poufnych w przypadku, gdy obowiązek ujawnienia Informacji poufnych wynikać będzie z powszechnie obowiązujących przepisów prawa bądź też z prawomocnego orzeczenia lub decyzji uprawnionego sądu lub organu. O każdorazowym powzięciu informacji o takim obowiązku Strona zobowiązania do ujawnienia Informacji poufnych będzie obowiązana do:

5. Zobowiązanie Współadministratorów do zachowania poufności w odniesieniu do Danych Osobowych powierzonych w związku z Umową lub Umową Podstawową jest nieograniczone w czasie i trwa niezależnie od rozwiązania lub wygaśnięcia Umowy i Umowy Podstawowej.

§ 11.
WYPOWIEDZENIE

1. Umowa zostaje zawarta na czas obowiązywania Umowy Podstawowej. W razie wątpliwości Umowa wygasa najpóźniej z momentem zakończenia obowiązywania Umowy Podstawowej.
2. Każdy Współadministrator jest uprawniony do rozwiązania Umowy ze skutkiem natychmiastowym na podstawie jednostronnego oświadczenia złożonego drugiemu Współadministratorowi na piśmie w przypadku rażącego lub powtarzającego się naruszenia Umowy przez drugiego Współadministratora, a także w przypadku gdy:
   1) organ nadzoru nad przestrzeganiem zasad przetwarzania Danych Osobowych stwierdzi, na podstawie prawomocnej decyzji, że Współadministrator lub Podmiot Przetwarzający, któremu ten Współadministrator powierzył przetwarzanie Danych Osobowych, nie przestrzega zasad przetwarzania Danych Osobowych;
   2) prawomocne orzeczenie sądu powszechnego wykaże, że Współadministrator nie przestrzega zasad przetwarzania Danych Osobowych.
3. Strony uzgadniają, że w przypadku rozwiązania niniejszej Umowy, Strona rozwiązująca będzie uprawniona do rozwiązania Umowy Podstawowej ze skutkiem natychmiastowym, jeżeli dla jej wykonania niezbędne jest przetwarzanie danych osobowych.

§ 12.
POSTANOWIENIA KOŃCOWE

1. Niniejsza Umowa stanowi regulację pomiędzy Współadministratorami, o której mowa w art. 26 ust. 1 RODO.
2. Postanowienia niniejszej Umowy zastępują wszelkie inne ustalenia dokonane pomiędzy Stronami dotyczące przetwarzania Danych Osobowych osób uprawnionych i są nadrzędne nad postanowieniami Umowy Podstawowej, o ile z postanowień Umowy Podstawowej nie wynika inaczej.
3. Wszelkie zmiany niniejszej Umowy wymagają formy pisemnej pod rygorem nieważności oraz muszą zostać podpisane przez osoby upoważnione do reprezentacji każdej ze Stron, z zastrzeżeniem wyjątków w niej przewidzianych.
4. W przypadku gdy którekolwiek z postanowień Umowy jest lub okaże się niezgodne z prawem, zostanie uznanie za nieważne lub nie mogące znaleźć zastosowania. Taka nieważność, niezgodność z prawem czy brak możliwości zastosowania postanowienia Umowy nie ma wpływu na pozostałe postanowienia Umowy, które zachowują swoją moc i winny być stosowane. Postanowienia nieważne winny być zastąpione przez nowe, zgodne z prawem, przy czym, nowa regulacja, w możliwie najszerszym zakresie winna oddawać pierwotnie założenia oraz cele handlowe zastępowanego postanowienia.

5. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

.....	.....
Administrator 1	Administrator 2

WZÓR

ZAŁĄCZNIK NR 12 DO
POLITYKI BEZPIECZEŃSTWA

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH[109]

NAZWA ORAZ DANE KONTAKTOWE ADMINISTRATORA: .....

Lp.	Nazwa czynności	Cele przetwarzania	Kategorie osób	Kategorie danych osobowych	Planowany termin usunięcia danych	Nazwa i dane kontaktowe współadministratora oraz przedstawiciela (jeśli dotyczy)	Nazwa i dane kontaktowe podmiotu przetwarzającego oraz przedstawiciela (jeżeli dotyczy)	Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe)	Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane	Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi
1.											
2.											
3.											
4.											
5.											
6.											
7.											

[109] Art. 30 ust. 1 RODO.

WZÓR

ZAŁĄCZNIK NR 13 DO
POLITYKI BEZPIECZEŃSTWA

REJESTR WSZYSTKICH KATEGORII CZYNNOŚCI PRZETWARZANIA[110]

Lp.	Nazwa kategorii czynności	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe)	Nazwa i dane kontaktowe administratora oraz przedstawiciela (jeżeli dotyczy)	Nazwa i dane kontaktowe współadministratora	Inspektor ochrony danych (jeżeli powołano)	Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane	Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi
1.							
2.							
3.							
4.							
5.							
6.							
7.							
8.							
9.							
10.							

[110] Art. 30 ust. 2 RODO.

WZÓR

ZAŁĄCZNIK NR 14 DO
POLITYKI BEZPIECZEŃSTWA

REJESTR BUDYNKÓW I POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

Lp.	Lokalizacja – adres	Precyzyjne określenie pomieszczenia	Dział/osoba użytkująca pomieszczenie	Zabezpieczenie pomieszczenia
1	2	3	4	5
1.	……..			
2.	……			
3.	……			

2021

WZÓR

ZAŁĄCZNIK NR 15 DO
POLITYKI BEZPIECZEŃSTWA

INWENTARYZACJA ZASOBÓW

Gminne Centrum Kultury i Sportu w Ostrowie	**Adres**	**Lokalizacja**	**Sprzęt komputerowy**	**Usługi telekomunikacyjne**	**Rodzaje zbiorów (T – tradycyjny, E – elektroniczny)**	**Dostęp (imię i nazwisko pracownika)**
OBSZARY PRZETWARZANIA (siedziba/y organizacji) pomieszczenia, w których przetwarzane są dane osobowe z uwzględnieniem lokalizacji, zasilania w energię elektryczną i sposobu jej rozprowadzenia, dostępu do usług telekomunikacyjnych, stref o różnych poziomach dostępu lub istotności przetwarzanych danych (np. pomieszczenia, w których znajduje się sprzęt komputerowy oraz te, w których go nie ma)						

Gminne Centrum Kultury i Sportu w Ostrowie	Architektura Sieci	Sposób Rozprowadzenia	Urządzenia Pośredniczące	Dostępność
SIEĆ TELEINFORMATYCZNA architektura sieci z uwzględnieniem sposobu jej rozprowadzenia (np. Ethernet, Wi-Fi, ADSL, wydzielone warstwy), użytych urządzeń pośredniczących (switch, router, hub itp.), a także innych urządzeń i rozwiązań zastosowanych w organizacji				

Gminne Centrum Kultury i Sportu w Ostrowie	Sprzęt	Producent I Model	Numer Ewidencyjny	Specyfikacja Techniczna	Osoba Odpowiedzialna
SPRZĘT serwery, komputery stacjonarne, komputery i inne urządzenia przenośne, nośniki danych, drukarki					

Gminne Centrum Kultury i Sportu w Ostrowie	Nazwa Dostawcy	Adres i Dane Kontaktowe	Oprogramowanie	Umowa, Licencja
OPROGRAMOWANIE począwszy od systemów operacyjnych (Windows, Linux), poprzez programy wspomagające zarządzanie (antywirus, firewall, zarządzanie kontami użytkowników, oprogramowanie monitorujące) oraz programy użytkowe i aplikacje biznesowe (edytory tekstu, arkusze kalkulacyjne, komunikatory, przeglądarki, programy pocztowe, programy księgowe, programy magazynowe, programy graficzne, projektowe, CRM, ERP itd.); należy pamiętać o dwóch rzeczach: inwentaryzacja oprogramowania musi objąć **również oprogramowanie bezpłatne,** a także do każdego programu powinniśmy posiadać licencję, aby zapewnić legalność jego użytkowania				