

Polityka Ochrony Danych Osobowych

w

Ośrodku Kultury w Mirosławcu



1	Wstęp	3
2	Analiza ryzyka	3
2.1	Definicje	3
2.2	Rejestr czynności przetwarzania (inwentaryzacja danych osobowych)	3
2.3	Wyznaczenie zagrożeń	4
2.4	Wyliczenie ryzyka dla zagrożeń	4
2.5	Plan postępowania z ryzykiem	5
3	Upoważnienia	5
4	Środki techniczne i organizacyjne zabezpieczające dane osobowe	5
5	Regulamin Ochrony Danych Osobowych	6
6	Instrukcja postępowania z incydentami	6

1 WSTĘP

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia

27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO).

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

2 ANALIZA RYZYKA

Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Przyjęto, że analiza ryzyka przeprowadzana jest dla zbioru lub grupy zbiorów (kategorii osób) lub dla procesów przetwarzania.

2.1 DEFINICJE

1. **Aktywa** – środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych.
2. **Naruszenie (Incydent) ochrony danych osobowych** - to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
3. **Zagrożenie** - potencjalne naruszenie (potencjalny incydent).
4. **Skutki** - rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia).
5. **Ryzyko** - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie aktywów.

2.2 REJESTR CZYNNOŚCI PRZETWARZANIA (INWENTARYZACJA DANYCH OSOBOWYCH)

Administrator będący równocześnie w stosunku do niektórych zbiorów Podmiotem przetwarzającym jest zobowiązany zgodnie z art. 30 RODO do prowadzenia rejestru czynności przetwarzania. Rejestr stanowi podstawę do przeprowadzenia analizy ryzyka.

1. Administrator prowadzi rejestr zgodnie z Załącznikiem nr 1 - Rejestr czynności przetwarzania (wykaz zbiorów danych osobowych).
2. Podmiot przetwarzający prowadzi rejestr zgodnie z Załącznikiem nr 2 - Rejestr czynności prowadzony przez Podmiot przetwarzający.

2.3 WYZNACZENIE ZAGROZEŃ

1. Administrator jest odpowiedzialny za określenie listy zagrożeń naruszenia poufności, dostępności i integralności, które mogą wystąpić podczas przetwarzania danych osobowych.
2. Zagrożenia powinny być identyfikowane w odniesieniu do uprzednio zinwentaryzowanych zbiorów (kategorii osób), aktywów oraz procesów przetwarzania.

2.4 WYLICZENIE RYZYKA DLA ZAGROZEŃ

1. Administrator określa Prawdopodobieństwo (P) wystąpienia poszczególnych zagrożeń w zbiorze (dla kategorii osób) lub w procesie przetwarzania.
2. Proponowaną skalę prawdopodobieństwa prezentuje Tabela A.
3. Administrator określa Skutki (S) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne.
4. Proponowaną Skalę skutków prezentuje Tabela B.
5. Administrator wylicza Ryzyka (R) dla wszystkich zagrożeń i ich skutków w/g formuły: $R = P * S$.

Tabela A PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA	SKALA (WAGA)
zagrożenie niskie	1
zagrożenie średnie	2
zagrożenie wysokie	3

Tabela B SKUTKI WYSTĄPIENIA ZAGROŻENIA	SKALA (WAGA)
małe (do 10000 PLN, incydent prasowy lokalny)	1
średnie (10000-100000 PLN, incydent prasowy ogólnopolski)	2
duże (od 100000 PLN, naruszenie prawa)	3

2.4.1 Porównanie wyliczonych ryzyk ze skalą i określenie dalszego postępowania z ryzykiem

1. Administrator porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem.
2. Proponowaną skalę Ryzyka prezentuje Tabela C.

Tabela C POZIOM RYZYKA	WARTOŚĆ [R = P*S]
ryzyko pomijalne i akceptowalne (akceptujemy)	1-2
ryzyko jest opcjonalne (akceptujemy albo obniżamy)	3-6
ryzyko jest nieakceptowalne (musimy obniżyć)	9

2.4.2 Reakcja na wartość ryzyka

1. Akceptacja ryzyka – zabezpieczenia są właściwe – brak potrzeby stosowania dodatkowych zabezpieczeń.
2. Działania obniżające ryzyko, które może zastosować Administrator:

- a. Przeniesienie –przerzucenie ryzyka (outsourcing, ubezpieczenie),
- b. Unikanie – eliminacja działań powodujących ryzyko.
3. Redukcja – zastosowanie zabezpieczeń w celu obniżenia ryzyka.
4. Analizę ryzyka przeprowadza się w specjalnym szablonie stanowiącym Załącznik nr 3 - Arkusz analizy ryzyka RODO natomiast stosowane zabezpieczenia wykazano w Załączniku nr 3a – Wykaz zabezpieczeń RODO.

2.4.3 Ponowna analiza ryzyka

Ponowna analiza ryzyka przeprowadzana jest cyklicznie lub po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów, nowych procesów przetwarzania, zmiany prawne).

2.5 PLAN POSTĘPOWANIA Z RYZYKIEM

1. Wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne, patrz Załącznik nr 4 - Plan postępowania z ryzykiem.
2. Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń.

3 UPOWAŻNIENIA

1. Administrator/podmiot przetwarzający odpowiada za nadawanie/anulowanie upoważnień do przetwarzania danych w zbiorach w postaci papierowej oraz w systemach informatycznych.
2. Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisu prawa.
3. Upoważnienia nadawane są do zbiorów na wnioski złożonych osób, zgodnie z zakresem obowiązków. Upoważnienia określają zakres operacji na danych, np. tworzenie, usuwanie, wgląd, przekazywanie – patrz Załącznik nr 5 - Upoważnienie do przetwarzania danych osobowych.
4. Administrator prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych. Patrz Załącznik nr 6 - Ewidencja osób upoważnionych.
5. W przypadku powierzenia przetwarzania danych do Podmiotu przetwarzającego, Administrator jest zobowiązany do sporządzenia z nim umowy powierzenia, stanowiącą podstawę upoważnienia dla osób z Podmiotu przetwarzającego - patrz Załącznik nr 7 - Umowa powierzenia.
6. Administrator prowadzi ewidencję umów powierzenia według Załącznika nr 8 – Rejestr umów powierzenia.

4 ŚRODKI TECHNICZNE I ORGANIZACYJNE ZABEZPIELAJĄCE DANE OSOBOWE

1. Administrator prowadzi wykaz zabezpieczeń, które stosuje w celu ochrony danych osobowych, patrz Załącznik nr 9 - Instrukcja zarządzania RODO.
2. W instrukcji wskazano stosowane zabezpieczenia proceduralne oraz zabezpieczenia jako środki techniczne i organizacyjne.
3. Instrukcja jest aktualizowana, jeśli zajdzie taka potrzeba po przeprowadzeniu analizy ryzyka.
4. Administrator opracował Politykę kluczy, która stanowi Załącznik nr 10 – Polityka kluczy.

5 REGULAMIN OCHRONY DANYCH OSOBOWYCH

Regulamin ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania. Patrz Załącznik nr 11 - Regulamin Ochrony Danych Osobowych.

Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania poprzez podpisanie oświadczenia o poufności stanowiącego Załącznik nr 12 – Oświadczenie o poufności.

6 INSTRUKCJA POSTĘPOWANIA Z INCYDENTAMI

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów, bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydu bezpośredniego przełożonego (lub jeśli jest powołany – Inspektora Ochrony Danych).
2. Do typowych podatności bezpieczeństwa danych osobowych należą:
 - a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
 - b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
 - c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
 - a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
 - b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twarde dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych),
 - c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
4. W przypadku stwierdzenia wystąpienia incydu, Administrator (lub w przypadku powołania – IOD) prowadzi postępowanie wyjaśniające w toku, którego:
 - a. ustala zakres i przyczyny incydu oraz jego ewentualne skutki,
 - b. inicjuje ewentualne działania dyscyplinarne,
 - c. działa na rzecz przywrócenia działań organizacji po wystąpieniu incydu,
 - d. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych, incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.

5. Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze – patrz Załącznik nr 13 - Formularz rejestracji incydentu.
6. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych.
7. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorcemu.

KLAUZULA INFORMACYJNA

- przetwarzanie danych na Facebook'u

Na podstawie art. 13 ust. 1 i ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679

z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych „RODO”) informujemy, że przetwarzamy Twoje dane osobowe. Szczegóły znajdziesz poniżej:

1. Administratorem Twoich danych osobowych jest Ośrodek Kultury w Mirosławcu z siedzibą przy ul. Parkowej 1 w Mirosławcu (78-650).

2. Powołaliśmy Inspektora Ochrony Danych, z którym możesz się skontaktować poprzez powyższy adres korespondencyjny oraz adres e-mail: iod.miroslawiec@wp.pl
Pamiętaj, iż powyższe dane służą wyłącznie do kontaktu w sprawach związanych bezpośrednio z przetwarzaniem danych osobowych.

3. Przetwarzanie Twoich danych osobowych odbywa się na podstawie art. 6 ust.1 lit. f RODO

- z uwagi, iż jest to niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora, tj. prowadzenia strony fanpage w portalu Facebook, przekazywania tą drogą informacji na temat produktów administratora danych osobowych oraz ustalenia, obrony i dochodzenia roszczeń z tym związanych.

4. W naszym prawnie usprawiedliwionym interesie leży dostarczanie informacji o wydarzeniach, które potencjalnie mogą zainteresować Społeczność, promocja naszej działalności poszerzanie grona naszych sympatyków a także utrzymywanie kontaktu ze wspomnianą Społecznością.

5. Poprzez funkcjonowanie naszego fanpage'a zbieramy i przetwarzamy następujące rodzaje danych osobowych:

- a) identyfikator Facebooka (zazwyczaj zawierający imię i nazwisko, które nie jest przez nas w jakikolwiek sposób weryfikowany w celu potwierdzenia prawdziwości danych);
- b) zdjęcie profilowe (dzięki niemu w niektórych przypadkach możemy poznać Twój

wizerunek);

c) inne zdjęcia (które również mogą przedstawiać wizerunek) wynikające z relacji fanpage - użytkownik. Umieszczanie zdjęć pod naszymi postami jest z Twojej strony dobrowolne;

d) treść Twoich komentarzy oraz treść rozmowy prowadzonej przez aplikację Messenger (dzięki niemu możemy dowiedzieć się o Twoim adresie e-mail, numerze telefonu oraz opisu, który zawarliście w związku z okolicznościami naszej korespondencji).

6. Dane osobowe zbierane poprzez komunikację z użytkownikami zostają przetwarzane tylko na potrzeby udzielenia odpowiedzi, jeśli istnieje taka konieczność.

7. Twoja aktywność związana z korzystaniem z naszego fanpage'a nie będzie archiwizowana poza serwisem Facebook.

8. Nie przekazujemy Twoich danych poza teren Polski/UE/ Europejskiego Obszaru Gospodarczego, jednak informujemy, że serwery serwisu Facebook znajdują się w Stanach Zjednoczonych Ameryki, gdzie obowiązują inne przepisy z zakresu ochrony danych osobowych, które w szczególności mogą nie zapewniać dostatecznego poziomu ochrony. Twoje dane zostaną przetransferowane przez serwis Facebook na jego serwery w celu stworzenia kopii zapasowej oraz w celach związanych z działalnością serwisu, a ponadto do wszystkich informacji o Użytkownikach ma dostęp Facebook a wszystkie interakcje na profilu Administratora są widoczne dla jego innych Użytkowników.

9. Dane osobowe Użytkowników są przechowywane przez okres obserwowania Profilu przez Użytkowników, a w uzasadnionych przypadkach przewidzianych odrębnymi przepisami prawa nie dłużej niż do czasu przedawnienia roszczeń.

10. Przysługuje Ci:

- a) prawo dostępu do swoich danych oraz otrzymania ich kopii,
- b) prawo do sprostowania swoich danych,
- c) prawo do usunięcia danych,
- d) ograniczenia przetwarzania danych,
- e) prawo do wniesienia sprzeciwu wobec przetwarzania danych,
- f) prawo do przenoszenia danych.

11. W sytuacji, gdy uznasz, że przetwarzanie podanych danych osobowych narusza przepisy RODO posiadasz prawo do wniesienia skargi do organu nadzorczego w

Polsce – Prezesa Urzędu Ochrony Danych Osobowych.

12. Twoje dane osobowe zostały pozyskane ze źródeł powszechnie dostępnych - z portalu Facebook.

Procedura projektowania nowych procesów

1. PRZEDMIOT / CEL

- 1.1 Niniejsza Procedura dotyczy każdego przypadku tworzenia nowego procesu związanego z przetwarzaniem danych osobowych.
- 1.2 Procedura wprowadzana jest celem wykazania, że jednostka przestrzega przepisów Rozporządzenia Parlamentu Europejskiego i Rady UE z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej „RODO”) przyjmując środki organizacyjne, które zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych.

2. ODPOWIEDZIALNOŚĆ

- 2.1. Nadzór nad aktualnością niniejszego dokumentu sprawuje Inspektor Ochrony Danych (IOD) przy wsparciu ze strony Informatyka jednostki.
- 2.2. W razie wątpliwości czy potrzeby konsultacji każdy zainteresowany pracownik jednostki ma obowiązek dokonać takiej konsultacji lub wyjaśnienia wątpliwości we współpracy z IOD.

3. TRYB POSTĘPOWANIA

- 3.1. Wymaga się, aby każdy właściciel projektowanego procesu, zanim dojdzie do jego wdrożenia i przed pozyskiwaniem danych osobowych, dokonał uprzedniej konsultacji z IOD lub ASI w szczególności pod kątem:
 - 3.1.1. ustalenia rodzaju przetwarzanych danych osobowych,
 - 3.1.2. ustalenia kategorii osób, których te dane dotyczą,
 - 3.1.3. ustalenia celów przetwarzania danych osobowych,
 - 3.1.4. potwierdzenia posiadania właściwej podstawy prawnej wynikającej z RODO do przetwarzania danych w ww. celach,
 - 3.1.5. w przypadku konieczności stosowania klauzul z zakresu ochrony danych osobowych – opracowania i wdrożenia ich treści,
 - 3.1.6. ustalenia miejsc przetwarzania danych osobowych,
 - 3.1.7. potwierdzenia, że zabezpieczenia danych osobowych są adekwatne do zagrożeń,
 - 3.1.8. w przypadku wykorzystywania systemu informatycznego służącego do przetwarzania danych osobowych – uzupełnienia i pozyskania wszystkich niezbędnych informacji dotyczących przygotowania technicznych środków zabezpieczeń, na podstawie pytań (Załącznik nr 1),
- 3.2. W każdym przypadku projektowania nowego procesu należy wziąć pod uwagę i zdefiniować proces biorąc pod uwagę w szczególności następujące kryteria:
 - 3.2.1. ilość zbieranych danych osobowych,
 - 3.2.2. okres ich przechowywania,
 - 3.2.3. dostępność,
 - 3.2.4. minimalizacja przetwarzania danych osobowych, rozumiana jako zbieranie danych osobowych wyłącznie w takim zakresie, jaki jest niezbędny do realizowania

zakładanych celów biznesowych. W przypadku sporządzania kopii dokumentów (np. dowodów tożsamości, praw jazdy czy innych) zwraca się uwagę na duże ryzyko naruszenia tej zasady, dlatego pracownicy zobowiązani są do powstrzymania się od utrwalania na kopii (papierowych bądź elektronicznych) danych osobowych w nadmiernym, nieadekwatnym zakresie,

- 3.2.5. jak najszybsza pseudonimizacja danych osobowych, gdzie to zasadne, rozumiana jako przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji. Warunkiem jest przechowywanie takich dodatkowych informacji osobno i zabezpieczenie ich w ten sposób, że niemożliwe jest przypisanie ich zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej,
- 3.2.6. przejrzystość co do funkcji i przetwarzania danych osobowych, co należy rozumieć jako zdefiniowanie i ustalenie roli danych osobowych dla procesu, jak też samych procesów przetwarzania (jak zbieranie, przechowywanie, udostępnianie, usuwanie, modyfikowanie, utrwalanie),
- 3.2.7. umożliwienie osobie, której dane dotyczą, monitorowania przetwarzania danych, co w szczególności oznacza zapewnienie poszanowania praw, które dotyczą danej osoby i wynikają z RODO, jak: prawo dostępu do treści danych i posiadania ich kopii, prawo do bycia zapomnianym (usunięcie danych), prawo do przenoszenia danych, prawo do wniesienia sprzeciwu, prawo do odwołania zgody na przetwarzanie danych,
- 3.2.8. umożliwienie administratorowi tworzenia i doskonalenia zabezpieczeń, w szczególności w przypadkach zmian (organizacyjnych, lokalowych, technicznych),
- 3.2.9. nadanie przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą.

4. SKUTKI PROCEDURY

- 4.1. Podjęcie decyzji o wdrożeniu projektowanego procesu jest zawsze w gestii Administratora Danych Osobowych.
- 4.2. Wdrożenie niniejszej Procedury skutkuje tym, że podjęcie takiej decyzji powinno być dokonane w oparciu o uprzednio:
 - 4.2.1. przeprowadzoną analizę procesu, zgodnie z założeniami Procedury oraz
 - 4.2.2. sformułowane wnioski wynikające z ww. analizy, oraz
 - 4.2.3. opinię przedstawioną przez IOD lub dodatkowo Informatyka.

**WYMAGANIA DLA SYSTEMU INFORMATYCZNEGO
SŁUŻĄCEGO DO PRZETWARZANIA DANYCH OSOBOWYCH**
biorąc pod uwagę wymagania RODO

1. Wymagania dotyczące uwierzytelniania

Jeżeli w systemie do logowania służy identyfikator i hasło, wymagania są następujące:

Lp.	Określenie wymogu	Czy wymóg spełniony	
		TAK	NIE
1.	System rejestruje dla każdego użytkownika odrębny identyfikator		
2.	Identyfikator użytkownika, który utracił uprawnienia, nie jest przydzielany innej osobie		
3.	Hasło do systemu informatycznego składa się co najmniej z 8 znaków		
4.	Hasło do systemu informatycznego składa się z małych i wielkich liter oraz cyfr lub znaków specjalnych		
5.	System nie posiada funkcji zapamiętania hasła, która umożliwi dostęp do systemu bez konieczności ponownego wprowadzania hasła		

2. Wymagania dotyczące funkcjonalności systemu

Lp.	Określenie wymogu	Czy wymóg spełniony	
		TAK	NIE
1.	System zapewnia automatycznie odnotowanie daty pierwszego wprowadzenia danych do systemu		
2.	System zapewnia automatycznie odnotowanie daty modyfikacji danych w systemie		
3.	System zapewnia automatycznie odnotowanie daty usunięcia danych w systemie		
4.	System zapewnia automatycznie odnotowanie identyfikatora użytkownika wprowadzającego dane do systemu		
5.	System zapewnia automatycznie odnotowanie identyfikatora użytkownika modyfikującego dane w systemie		
6.	System zapewnia automatycznie odnotowanie identyfikatora użytkownika usuwającego dane w systemie		
7.	System zapewnia odnotowanie źródła danych, jeżeli dane pochodzą nie od osoby, której dotyczą, np. zbierane są z CEIDG, z LinkedIn, zakup bazy danych - automatycznie lub ręcznie przez użytkownika		

8.	System zapewnia odnotowanie informacji o odbiorcach ¹ , którym dane zostały udostępnione - automatycznie lub ręcznie przez użytkownika		
9.	System zapewnia odnotowanie informacji o dacie udostępnienia danych odbiorcom, którym dane zostały udostępnione - automatycznie lub ręcznie przez użytkownika		
10.	System zapewnia odnotowanie informacji o zakresie danych, które zostały udostępnione odbiorcom - automatycznie lub ręcznie przez użytkownika		
11.	System zapewnia odnotowanie, jaka zgoda została wyrażona (np. wydzielenia pola przy rekordzie w systemie z opisem, czego zgoda dotyczy) - automatycznie lub ręcznie przez użytkownika		
12.	System zapewnia odnotowanie, kiedy dana zgoda została wyrażona - automatycznie lub ręcznie przez użytkownika		
13.	System zapewnia odnotowanie, kiedy dana zgoda została odwołana - automatycznie lub ręcznie przez użytkownika		
14.	System zapewnia odnotowanie informacji o dacie wniesienia sprzeciwu wobec przetwarzania danych osobowych - automatycznie lub ręcznie przez użytkownika		
15.	System zapewnia edycję danych (ich aktualizację)		
16.	System zapewnia możliwość przetwarzania danych w formie ich archiwizacji		
17.	System zapewnia możliwość trwałego usunięcia danych		
18.	System zapewnia możliwość odnotowania, że osoba, której dane dotyczą, wniosła o ograniczenie ich przechowywania (tzn. wyłącznie do ich przechowywania)		
19.	System umożliwia dostarczenie osobie, której dane dotyczą, jej własnych danych osobowych, w powszechnie używanym, ustrukturyzowanym formacie nadającym się do odczytu maszynowego		
20.	System umożliwia przesłanie danych osobowych konkretnej osoby bezpośrednio podmiotowi, któremu ona wskaże, w powszechnie używanym, ustrukturyzowanym formacie nadającym się do odczytu maszynowego		

3. Wymagania dotyczące zabezpieczenia technicznego i fizycznego

Lp.	Określenie wymogu	Czy wymóg spełniony	
		TAK	NIE
1.	Baza danych systemu jest szyfrowana		
2.	Dostęp do danych osobowych jest zabezpieczony poprzez pseudonimizację (użycie w miejsce jednego atrybutu np. rzeczywistego imienia i nazwiska, innego atrybutu (np. inicjału, liczby), by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji. Te dodatkowe informacje powinny być przechowywane osobno i objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie określonej osobie fizycznej), np. szyfrowanie kluczem tajnym, funkcja skrótu, tokenizacja)		
3.	Dyski urządzeń przenośnych z zapisem danych osobowych są szyfrowane		

¹ Odbiorcami, których **nie dotyczy** odnotowanie udostępnienia są: osoby, których dane dotyczą, osoby upoważnione do przetwarzania danych w Spółce (zwłaszcza pracownicy), podmioty, z którymi Spółka ma podpisane umowy powierzenia (dostawcy usług - procesorzy), organy publiczne (państwowe lub organy samorządu terytorialnego), którym dane są udostępniane na podstawie przepisów prawa (np. ZUS, US, sądy, prokuratura, Policja, komornik). Odbiorcą może być np. ubezpieczyciel

4.	Możliwe jest zablokowanie urządzenia lub usunięcie jego zawartości - na odległość, w razie zgubienia lub utraty		
5.	Tworzone są kopie zapasowe		
6.	Zapis kopii zapasowych danych nie jest przechowywany w pomieszczeniu, gdzie znajduje się serwer, z którego one pochodzą		
7.	Zapewnia się poufność danych przetwarzanych w systemie		
8.	Zapewnia się integralność danych przetwarzanych w systemie		
9.	Zapewnia się dostępność danych przetwarzanych w systemie		
10.	Zapewnia się odporność systemu na zagrożenia wpływające w szczególności na utratę, zabranie, nieuprawnione ujawnienie lub modyfikację, uszkodzenie danych		
11.	Zapewnia się zdolność do szybkiego przywracania dostępności danych osobowych i dostępu do nich w razie incydentu		
12.	Stosuje się regularne testowanie, mierzenie i ocenianie skuteczności zabezpieczeń systemu		
13.	Serwer, na którym przetwarzane są dane osobowe przechowywany jest w miejscu fizycznie zabezpieczonym przed utratą danych spowodowaną np. pożarem, zalaniem, włamaniem		
14.	Nośniki kopii zapasowych, na których przetwarzane są dane osobowe przechowywane są w miejscu fizycznie zabezpieczonym przed utratą danych spowodowaną np. pożarem, zalaniem, włamaniem		
15.	Komputery, na których przetwarzane są dane osobowe przechowywane są w miejscu fizycznie zabezpieczonym przed utratą danych spowodowaną np. pożarem, zalaniem, włamaniem, nieuprawnionym wglądem, kradzieżą		
16.	Każdy użytkownik posiada odrębne login+hasło do swojego konta (zarówno w przypadku profili na komputerze, jak i dedykowanych systemach informatycznych)		

100

100

100