Spis treści

1. PRZEDMIOT / CEL

1.1. Niniejszy dokument reguluje sposób przeprowadzenia dwóch rodzajów ocen ryzyka:

a) Analizy ryzyka dla poszczególnych procesów przetwarzania danych osobowych jakie zachodzą w NRA zgodnie z art. 24 ust. 1 RODO;

b) Oceny skutków dla ochrony danych osobowych (DPIA) zgodnie z art. 35 RODO.

1.2. Celem przeprowadzenia analizy ryzyka jest:

a) zapewnienie zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania danych osobowych,

b) definiowanie i wdrożenie odpowiednich środków technicznych i organizacyjnych, zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku,

c) dokonanie oceny czy stopień bezpieczeństwa jest odpowiedni, z uwzględnieniem ryzyka wiążącego się z przetwarzaniem danych osobowych, w szczególności wynikającym z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do przetwarzanych danych osobowych, co mogłoby skutkować naruszeniem praw i wolności osób, których dane dotyczą.

1.3. Celem oceny skutków dla ochrony danych osobowych jest scharakteryzowanie przetwarzania danych, dokonanie oceny jego niezbędności i proporcjonalności oraz wsparcie administratora w zarządzaniu ryzykiem naruszenia praw lub wolności osób fizycznych wynikającym z tego przetwarzania.

1.4. W niniejszym dokumencie mają zastosowanie terminy zdefiniowane w Polityce Ochrony Danych Osobowych.

2. ODPOWIEDZIALNOŚĆ

2.1. Nadzór nad aktualnością niniejszego dokumentu sprawuje Dyrektor Biura NRA przy wsparciu ze strony Inspektora Ochrony Danych (IOD).

2.2. Za przeprowadzenie oceny ryzyka każdorazowo odpowiedzialny jest właściciel biznesowy procesu przetwarzania danych osobowych, który ma być poddany takiej ocenie.

Przykład 1: w przypadku procesu przetwarzania danych na potrzeby kadrowe właścicielem biznesowym będzie kierownik jednostki organizacyjnej odpowiedzialnej za sprawy kadrowe.

Przykład 2: w przypadku procesu przetwarzania danych polegającego na gromadzeniu plików cookies i poddawaniu ich analizie pod kątem marketingowym właścicielem biznesowym będzie kierownik jednostki organizacyjnej odpowiedzialnej za marketing.

2.3. W ramach oceny ryzyka oraz DPIA rekomendacje do procesu zgłaszają:

a) Dyrektor Działu IT,

b) IOD.

2.4. Ostateczna akceptacja ryzyka leży wyłącznie w gestii właściciela biznesowego.

2.5. Wypełnione arkusze przechowują właściciele biznesowi przypisani do ocenianego w ten sposób procesu przetwarzania danych.

Ocena ryzyka powinna być procesem ciągłym oraz podlegającym cyklicznej aktualizacji w przypadku zaistniałej potrzeby jej przeprowadzenia, biorąc pod uwagę zmieniające się okoliczności oraz pojawiające się nowe podatności i zagrożenia dla praw i wolności osób fizycznych.

3. TRYB POSTĘPOWANIA – ANALIZA RYZYKA

Rozdział 1. ZASADY OGÓLNE, UCZESTNICY

§ 1.

Informacje o analizowanym procesie przetwarzania danych osobowych pobierane są z Rejestru Czynności Przetwarzania Danych NRA W razie potrzeby w toku realizacji procesu analizy ryzyka, właściciel biznesowy udziela uczestnikom procesu analizowani ryzyka dodatkowych informacji. Jeżeli analiza ryzyka ma dotyczyć planowanego procesu, niezbędne informacja dostarcza właściciel biznesowy.

§ 2.

Na każdym etapie zarządzania ryzykiem dla ochrony danych osobowych zaangażowane są wszystkie strony zainteresowane:

a) Prezydium NRA,
b) właściciel biznesowy,
c) IOD,
d) Dyrektor Działu IT,
e) pracownicy uczestnicząc w procesie,
f) podmioty przetwarzające dane osobowe w imieniu i na zlecenie NRA (jeżeli zachodzi taka konieczność).

Rozdział 2. ELEMENTY SKŁADOWE OCENY RYZYKA

§ 3.

1. Ryzyko dla ochrony danych osobowych jest szacowane metodą ilościowo-jakościową zgodnie z rekomendacjami normy PN-EN ISO/IEC 27005.
2. Ocena ryzyka składa się z trzech elementów:
   a) oceny prawdopodobieństwa wystąpienia ryzyka w pięciopunktowej skali tj.: rzadkie – mało prawdopodobne – możliwe – prawdopodobne – prawie pewne,
   b) oceny konsekwencji naruszenia dla Administratora w pięciopunktowej skali tj.: bardzo małe – małe – średnie – duże – bardzo duże,
   c) ostatecznej oceny ryzyka w czteropunktowej skali tj.: niskie – średnie – wysokie – krytyczne.
3. Ocenę ryzyka należy wykonać dla dwóch sytuacji – przed uwzględnieniem rekomendacji ze strony IOD oraz Działu IT, a także środków, które sam właściciel biznesowy jest w stanie wskazać w celu minimalizacji ryzyka oraz po uwzględnieniu ww. rekomendacji. Ocena ryzyka dla ww. sytuacji odbywa się równocześnie. W ten sposób właściciel biznesowy będzie mógł zweryfikować, jak na ryzyko będą przekładać się działania je minimalizujące, czyli wdrażanie rekomendacji. Wdrażanie rekomendacji stanowi podstawową formę postępowania z ryzykiem.
4. Ocena ryzyka może być realizowana przy użyciu szablonu, którego wzór stanowi **Załącznik A**. do niniejszego dokumentu.

Rozdział 3. OCENA PRAWDOPODOBIEŃSTWA WYSTĄPIENIA RYZYKA

§ 4.

1. Poprzez **prawdopodobieństwo** należy rozumieć miarę służącą do opisu częstości lub pewności zmaterializowania się danego ryzyka, wywierającego wpływ działalność Administratora.
2. Prawdopodobieństwo oceniamy zgodnie z powyższym, korzystając z pięciostopniowej skali:
   1.2.1. rzadkie – minimalna szansa wystąpienia zagrożenia (współczynnik: 1),
   1.2.2. mało prawdopodobne – zagrożenie jest realne, nie wystąpiło w NRA, ale wystąpiło w innych organizacjach (współczynnik: 2),
   1.2.3. możliwe – zagrożenie jest możliwe, wystąpiło w NRA raz (współczynnik: 3),
   1.2.4. prawdopodobne – zagrożenie jest prawdopodobne, wystąpiło w NRA więcej niż raz (współczynnik: 4),
   1.2.5. prawie pewne – zagrożenie jest prawie pewne, wiele razy wystąpiło w NRA przy realizacji zadań, a podjęte środki zaradcze okazywały się niewystarczające (współczynnik: 5).
3. Szacując prawdopodobieństwo, należy wziąć pod uwagę fakt, czy opisywane zagrożenie ziściło się w NRA (patrz: opisy do pięciostopniowej skali).

Rozdział 4. OCENA KONSEKWENCJI NARUSZENIA DLA ADMINISTRATORA

§ 5.

1. Poprzez **wpływ** należy rozumieć skutek oddziaływania zmaterializowanego ryzyka na NRA; wpływ ryzyka na prawa lub wolności osoby, której dane dotyczą może być rzadki, mało prawdopodobny, możliwy, prawdopodobny bądź prawie pewny.
2. Wpływ jest oceniamy w pięciostopniowej skali, która uwzględnia konsekwencje majątkowe oraz niemajątkowe (dla reputacji NRA). Dla potrzeb analizy ryzyka należy wybierać bardziej dotkliwy z dwóch skutków):

a) bardzo małe – naruszenie danych bez szkody finansowej i reputacyjnej (współczynnik: 1),

b) małe – naruszenie danych ze szkodą w zakresie 5-50 tys. zł, negatywne opinie bez udziału mediów (współczynnik: 2),

c) średnie – naruszenie danych ze szkodą w zakresie 50-250 tys. zł, negatywne opinie w mediach lokalnych (współczynnik: 3),

d) duże – naruszenie danych ze szkodą w zakresie 250-500 tys. zł, negatywne opinie w mediach krajowych (współczynnik: 4),

e) bardzo duże – katastrofalne naruszenie danych ze szkodą w zakresie powyżej 500 tys. zł, negatywne opinie w mediach międzynarodowych (współczynnik: 5).

Rozdział 5. OCENA POZIOMU RYZYKA. POSTĘPOWANIE Z RYZYKIEM.

§ 6.

1. Ocena poziomu ryzyka (R) wykonywana jest zgodnie z poniższym równaniem:

$$R = P \times W$$

P – prawdopodobieństwo
W – wpływ

2. Określenie poziomu ryzyka dokonuje się poprzez wprowadzenie w arkuszu oceny ryzyka przyjętych wartości prawdopodobieństwa i wpływu dla poszczególnych zagrożeń (od 1 do 5), po czym arkusz automatycznie dokonuje wyliczenia poziomu ryzyka.
3. Przyjmuje się następujące poziomy ryzyka dla następujących wartości iloczynu prawdopodobieństwa i wpływu:
   a) Niski: 1 – 3,
   b) Średni: 4 – 7,
   c) Wysoki: 8-12,
   d) Krytyczny: 13-25.

§ 7.

1. Właściciel biznesowy podejmuje działania naprawcze w ramach postępowania z ryzykiem dla praw i wolności osób, których dane dotyczą. Działania te zależne są od powagi ryzyka oraz możliwości technicznych i finansowych NRA.
2. Właściciel biznesowy podejmuje następujące działania w ramach postępowania z ryzykiem:
   a) dokonuje jego akceptacji bez konieczności wdrażania dodatkowych działań (ryzyko niskie),
   b) dokonuje jego akceptacji po wdrożeniu dodatkowych działań (po uzyskaniu akceptacji ze strony IOD oraz Działu IT, lecz jednocześnie stale monitoruje ryzyko (ryzyko średnie),
   c) redukuje ryzyko poprzez odpowiednie działania mające na celu poprawę zabezpieczeń technicznych i/lub organizacyjnych (ryzyko średnie, wysokie i krytyczne),
   d) unika ryzyka – podejmuje decyzję o zaprzestaniu przetwarzania danych (na etapie projektowania przetwarzania danych lub ich rzeczywistego przetwarzania, jeżeli pomimo podejmowanych działań, o których mowa w w/w punktach nie udało się obniżyć ryzyka do poziomu 12 lub mniej).
3. Odstępstwo od zasad przewidzianych w ust. 2 powyżej, czyli decyzja biznesowa sprzeczna z procedurą, jest ryzykiem wyłącznie biznesowym NRA.

Rozdział 6. PLAN ZARZĄDZANIA RYZYKIEM

§ 8.

Właściciel biznesowy obszaru, w ramach którego zidentyfikowane zostało ryzyko nieakceptowalne (§ 7 ust. 2 c) oraz d) powyżej), opracowuje **plan zarządzania ryzykiem**, który określa w szczególności:

a) działania, jakie zostaną podjęte w celu zaradzenia ryzyku,
b) opis mechanizmów, jakie powstaną w wyniku realizacji tego planu (zarówno w sferze organizacyjnej, jak i technologicznej),

c) mierniki oceny skuteczności realizacji planu – wskaźniki, na podstawie których oceniana będzie skuteczność wdrażanych środków zaradczych mających na celu obniżenie ryzyka do akceptowalnego poziomu,

d) osobę lub osoby odpowiedzialne za realizację działań zaradczych,

e) termin realizacji działań zaradczych.

§ 9.

1. Plan zarządzania ryzykiem ma zastosowanie do wszystkich obszarów ryzyka nieakceptowalnego.
2. Plan związany jest bezpośrednio z procesem zarządzania ryzykiem. Wskazuje on sposób postępowania z ryzykiem i jest zatwierdzany przez właściciela biznesowego. W przypadku niezaakceptowania zidentyfikowanego ryzyka, właściciel biznesowy określa działania korygujące niezbędne do jego eliminacji. Plan zarządzania ryzykiem jest nieodłącznym elementem doskonalenia i utrzymywania bezpieczeństwa przetwarzania danych osobowych w NRA.
3. Każde opracowanie planu prezentowane jest w formie tabelarycznej, gdzie poszczególne kolumny tabeli oznaczają:
   a) **Nazwa procesu/zasobu** – nazwa ryzyka, z którym związane jest dane działanie korygujące;
   b) **Właściciel biznesowy** – wskazanie właściciela zidentyfikowanego ryzyka;
   c) **Opis podatności – możliwe straty**, które mogą wynikać z podjętych działań lub zachodzących losowych zdarzeń mających przełożenie na wystąpienie zagrożenia;
   d) **Poziom ryzyka (wynik analizy ryzyka) -** określenie poziomu ryzyka, dokonywanego poprzez wprowadzenie w arkuszu oceny ryzyka przyjętych wartości prawdopodobieństwa i wpływu dla poszczególnych zagrożeń;
   e) **Sposób postępowania**– decyzja właściciela biznesowego w oparciu o możliwości wskazane w § 7 ust. 2;
   f) **Środki planowane w celu zaradzeniu ryzyka** – sposób wdrożenia w życie danego działania korygującego;

g) **Wymagania normy ISO / przepis RODO** – wymagania, na których ocenę wpływa stosowanie normy ISO (wymagania normy ISO/IEC 27001, ISO/IEC 27005, których ocena spełnienia wzrośnie po wdrożeniu działania korygującego) lub wymagania, na których ocenę wpływa stosowanie przepisu RODO;

h) **Data wdrożenia działania korygującego** – przewidywany czas niezbędny dla wdrożenia w życie danego działania korygującego, zapoznanie się pracowników z procedurami, instrukcjami, ewentualne szkolenia etc. Jest to czas od chwili zatwierdzenia danego działania do chwili, gdy zacznie ono funkcjonować zgodnie z oczekiwaniami, czyli gdy jego działanie zostanie ocenione pozytywnie w czasie audytu;

i) **Efekt działania** – oczekiwany efekt po zakończeniu realizacji działań korygujących;

j) Ryzyka **zaakceptowane przez właściciela biznesowego** – ryzyka akceptowalne przez biznes;

4. Opracowania Planu zarządzania ryzykiem, zawierającego m.in. zestawienia ryzyk wraz z opisem działań korygujących oraz szacowaną datą wdrożenia, dokonuje się w formie tabelarycznej zgodnie z **Załącznikiem B** do niniejszej procedury.

4. TRYB POSTĘPOWANIA - DPIA

Rozdział 6: ZASADY OGÓLNE DPIA, UCZESTNICY

§ 10.

DPIA jest obowiązkowo przeprowadzana w następujących sytuacjach:

1. Jeżeli dany rodzaj przetwarzania – 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, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych (art. 35 ust. 1 RODO),
2. Jeżeli dany rodzaj przetwarzania wiąże się z:
   a) systematyczną, kompleksową oceną 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;

b) przetwarzaniem na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO, lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o czym mowa w art. 10 RODO;

c) systematycznym monitorowaniem na dużą skalę miejsc dostępnych publicznie.

3. Jeżeli dany rodzaj przetwarzania jest wymieniony w Komunikacie Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (M. P. z 2019 r. poz. 666).

§ 11.

Informacje o analizowanym w ramach DPIA procesie przetwarzania danych osobowych opracowywane są przez właściciela biznesowego procesu we współpracy z IOD. W razie potrzeby w toku realizacji procesu analizy ryzyka, właściciel biznesowy udziela uczestnikom procesu analizowani ryzyka dodatkowych informacji.

§ 12.

Na każdym etapie tworzenia DPIA zaangażowane są wszystkie strony zainteresowane:

a) Prezydium NRA

b) właściciel biznesowy,

c) IOD,

d) Dyrektor Działu IT,

e) pracownicy uczestniczący w procesie,

f) podmioty przetwarzające dane osobowe w imieniu i na zlecenie NRA (jeżeli zachodzi taka konieczność).

Rozdział 7: ELEMENTY SKŁADOWE DPIA

§ 13.

1. DPIA składa się z dwóch zasadniczych elementów:

a) Opisu planowanego procesu przetwarzania

b) Oceny ryzyka, w trakcie której przeprowadza się:

- ocenę prawdopodobieństwa wystąpienia ryzyka w pięciopunktowej skali tj.: rzadkie – mało prawdopodobne – możliwe – prawdopodobne – prawie pewne,
- oceny wpływu ryzyka na prawa lub wolności osoby, której dane dotyczą w pięciopunktowej skali tj.: bardzo małe – małe – średnie – duże – bardzo duże,
- ostatecznej oceny wpływu ryzyka całościowego na prawa lub wolności osoby, której dane dotyczą w czteropunktowej skali tj.: niskie – średnie – wysokie – krytyczne.

2. Szablon analizy DPIA zawarto w **Załączniku C** do niniejszego dokumentu.

3. Ryzyka występujące w arkuszu oceny ryzyka podzielono na:

a) ryzyka prawne,

b) ryzyka z zakresu bezpieczeństwa danych tj. czynniki organizacyjne, logiczne (informatyczne/IT) oraz fizyczne.

ZAŁĄCZNIKI

- Załącznik A – Wzór arkusza analizy ryzyka.
- Załącznik B – Wzór planu postępowania z ryzykiem.
- Załącznik C – Wzór arkusza DPIA.

5. TABELA ZMIAN

L.p.	Numer wydania dokumentu	Miejsce zmiany (nr punktu)	Opis zmiany	Nowy numer wydania dokumentu	Wprowadzający zmiany	
					Data	Imię i Nazwisko
	2		Zmiana polega na aktualizacji i weryfikacji aktualności tego dokumentu oraz na stworzeniu nowej treści dokumentu obejmującego załączniku w postaci arkuszu oceny ryzyka, postępowania z ryzykiem oraz DPIA	2	27.01.2025 r.	

Załącznik nr 1

do Procedury projektowania nowych procesów

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, 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		
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)		

4. Inne zabezpieczenia o charakterze fizycznym, technicznym, organizacyjnym

Lp.	Pytanie	Odpowiedź	
		TAK	NIE
1.	Czy istnieją procedury zarządzania nośnikami wymiennymi, zawierającymi dane osobowe?		
2.	Czy nośniki, które nie będą dłużej wykorzystywane, są bezpiecznie wycofane, zgodnie z formalnymi procedurami?		
3.	Czy nośniki zawierające dane osobowe są chronione przed nieuprawnionym dostępem, nadużyciem oraz utratą integralności podczas transportu?		

4.	Czy użytkownicy mają dostęp wyłącznie do tych sieci i usług sieciowych, do których otrzymali wyraźne uprawnienie?		
5.	Czy wdrożono formalny proces rejestrowania i wyrejestrowywania użytkowników?		
6.	Czy wdrożono formalny proces przydzielania dostępu użytkownikom w celu nadawania lub odbierania praw dostępu do wszystkich systemów wszystkim kategoriom użytkowników?		
7.	Czy wprowadzono mechanizmy ograniczenia i nadzoru przydzielania i wykorzystywania praw dostępu?		
8.	Czy przydzielanie poufnych informacji uwierzytelniających podlega formalnemu procesowi zarządzania?		
9.	Czy administrator przegląda prawa dostępu użytkowników w regularnych odstępach czasu?		
10.	Czy przydzielone pracownikom i użytkownikom zewnętrznym prawa dostępu do informacji i środków przetwarzania informacji są odbierane po zakończeniu zatrudnienia, umowy lub porozumienia lub dostosowywane do zaistniałych zmian?		
11.	Czy sprzęt został umieszczony i chroniony w taki sposób by zredukować ryzyko wynikające z zagrożeń i niebezpieczeństw środowiskowych oraz okazji do nieuprawnionego dostępu?		
12.	Czy sprzęt chroniony jest przed awariami zasilania oraz innymi przerwami spowodowanymi awariami systemów wspomagających?		
13.	Czy okablowanie zasilające oraz telekomunikacyjne przenoszące dane lub wspomagające usługi informacyjne jest chronione przed przechwyceniem, zakłóceniem lub uszkodzeniem?		
14.	Czy sprzęt jest prawidłowo konserwowany w celu zapewnienia jego ciągłej dostępności i integralności?		
15.	Czy sprzęt jest wynoszony poza siedzibę organizacji po uzyskaniu wcześniejszego zezwolenia?		
16.	Czy sprzęty wynoszone poza siedzibę organizacji są zabezpieczone przed wystąpieniem różnych ryzyk związanych z pracą poza siedzibą?		
17.	Czy przed zbyciem lub przekazaniem sprzętu do ponownego użycia sprawdzane są wszystkie jego składniki zawierające dane osobowe, dla		

	zapewnienia, że wszystkie takie dane zostały usunięte lub bezpiecznie nadpisane?		
18.	Czy użytkownicy zapewniają odpowiednią ochronę sprzętu pozostawionego bez opieki?		
19.	Czy wprowadzono politykę czystego biurka dla dokumentów papierowych i przenośnych nośników pamięci oraz politykę czystego ekranu dla środków przetwarzania danych osobowych?		
20.	Czy wdrożone zostały zabezpieczenia wykrywające, zapobiegające i odtwarzające, które służą ochronie przed szkodliwym oprogramowaniem?		
21.	Czy zapasowe kopie informacji, oprogramowania i obrazów systemu są regularnie wykonywane i testowane zgodnie z ustaloną polityką kopii zapasowych?		
22.	Czy tworzone, przechowywane i systematycznie przeglądane są dzienniki zdarzeń rejestrujące działania użytkowników, wyjątki, usterki oraz zdarzenia związane z bezpieczeństwem informacji?		
23.	Czy środki służące rejestrowaniu zdarzeń oraz informacje w dziennikach zdarzeń chronione są przed manipulacją i nieuprawnionym dostępem?		
24.	Czy działanie administratorów i operatorów systemów są rejestrowane a dzienniki chronione i systematycznie przeglądane?		
25.	Czy zegary wszystkich istotnych systemów przetwarzania informacji w organizacji lub domenie bezpieczeństwa są zsynchronizowane z jednym wzorcowym źródłem czasu?		
26.	Czy wdrożono procedury nadzoru nad instalacją oprogramowania w systemach produkcyjnych?		