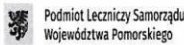


**DOKUMENTACJA ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA SZPITALA SPECJALISTYCZNEGO W PRABUTACH SP. Z O.O.**

Szpital Specjalistyczny w Prabutach sp. z o.o.   Podmiot Leczniczy Samorządu Województwa Pomorskiego	PROCEDURA	Wydanie: 3	<b>10.08.2025</b>
			Strona 1 z 81
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

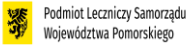
	IMIĘ I NAZWISKO / STANOWISKO	DATA	INSPEKTOR Ochrony Danych Osobowych
<b>OPRACOWAŁ</b>	Edmund Preuss <b>IODO</b>	<b>10.08.2025</b>	<i>mgr Edmund Preuss</i>
<b>SPRAWDZIŁ</b>	Łukasz Brzoza <b>Informatyk</b>	<b>10.08.2025</b>	<i>Łukasz Brzoza</i>
<b>ZATWIERDZIŁ</b>	Grażyna Stachowicz <b>Prezes Zarządu</b>	<b>10.08.2025</b>	<b>PREZES ZARZĄDU</b> <i>Grażyna Stachowicz</i>

**HISTORIA ZMIAN DOKUMENTU**

Data wydania	Nr wydania	Opis zmiany
	1	Pierwsze wydanie procedury
01.09.2022	2	Aktualizacja procedury
10.08.2025	3	Aktualizacja procedury oraz zmiana numeru (7- Pr5, QP-ZI-1, QP-ZI 1.1, QP-ZI-2, QP-ZI-3.5)



**Spis treści**

1.	Postanowienia ogólne.....	4
1.1.	Przedmiot.....	4
1.2.	Terminologia i określenia.....	5
1.3.	Cel i strategię bezpieczeństwa.....	6
1.4.	Zasady dotyczące przetwarzania danych osobowych [5].....	7
1.5.	Zgodność przetwarzania z prawem [6].....	7
1.6.	Przetwarzanie szczególnych kategorii danych osobowych [9].....	9
1.7.	Przetwarzanie danych osobowych w miejscu pracy.....	11
2.	Odpowiedzialność.....	18
2.1.	Administrator Danych Osobowych [24].....	18
2.2.	Inspektor ochrony danych [37-39].....	21
2.3.	Użytkownik (kierownik komórki organizacyjnej, pracownik).....	24
2.4.	Odpowiedzialność Administratora Systemów Informatycznych.....	25
2.5.	Odpowiedzialność ADO jako Podmiotu Przetwarzającego [28].....	26
3.	Prawa osób, których dane są przetwarzane.....	28
3.1.	Obowiązki informacyjne.....	29
3.1.1.	Przejrzyste informowanie i przejrzysta komunikacja oraz tryb wykonywania praw przez osobę, której dane dotyczą [12].....	29
3.1.2.	Obowiązek informacyjny odnośnie prawa do sprzeciwu [21].....	31
3.1.3.	Klauzula Informacyjna [13-14].....	29
3.1.4.	Zgoda na przetwarzanie danych osobowych [7].....	36
3.2.	Prawo dostępu przysługujące osobie, której dane dotyczą [15].....	42



<p>Szpital Specjalistyczny w Prabutach sp. z o.o.</p>  <p>Podmiot Leczniczy Samorządu Województwa Pomorskiego</p>	<p><b>PROCEDURA</b></p>	Wydanie: 3	<b>10.08.2025</b>
		Strona 2 z 81	
<p><b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b></p>		<p>Nr dokumentu: <b>7- Pr5</b></p>	

3.3.	Prawo do sprostowania danych [16].....	43
3.4.	Prawo do usunięcia danych („prawo do bycia zapomnianym”) [17].....	44
3.5.	Prawo do ograniczenia przetwarzania [18] .....	45
3.6.	Prawo do przenoszenia danych [20] .....	46
3.7.	Prawo do sprzeciwu [21] .....	52
3.8.	Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie [22] .....	54
4.	Naruszenia ochrony danych osobowych [33 i 34] .....	56
5.	Ocena skutków dla ochrony danych [35] .....	57
6.	Uprzednie Konsultacje [36] .....	59
7.	Zarządzanie ryzykiem w systemie ochrony danych osobowych.....	60
8.	Powierzenie danych osobowych [28].....	60
9.	Obszar przetwarzania danych osobowych.....	61
10.	Rejestrowanie czynności przetwarzania [30] .....	61
11.	Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych [32] .....	64
11.1.	Środki ochrony fizycznej.....	64
11.2.	Środki sprzętowe, informatyczne i telekomunikacyjne.....	65
11.3.	Środki ochrony w ramach oprogramowania systemu .....	65
11.4.	Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych ...	66
11.5.	Środki ochrony w ramach systemu użytkowego .....	66
11.6.	Środki organizacyjne .....	66
11.7.	Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych .....	66
ZASADY POSTĘPOWANIA DLA PRACOWNIKÓW :.....		67
12.	Sprawdzanie systemu ochrony danych osobowych [39].....	68
13.	Procedura postępowania w przypadku naruszenia bezpieczeństwa systemu ochrony danych osobowych [33] .....	70
14.	Zarządzanie systemami informatycznymi, w których przetwarzane są dane osobowe.....	72
14.1.	Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności .....	72
14.2.	Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem.....	73
14.3.	Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.....	73
14.4.	Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.....	74
14.5.	Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe.....	75

**DOKUMENTACJA ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA SZPITALA SPECJALISTYCZNEGO W PRABUTACH SP. Z O.O.**

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Lecznicy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Strona 3 z 81	
		Nr dokumentu: <b>7- Pr5</b>	

14.6.	Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania złośliwego.....	75
14.7.	Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.....	76
15.	Postanowienia końcowe.....	77
16.	Załączniki.....	77

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Lecznicy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
			Strona 4 z 81
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

## 1. Postanowienia ogólne

### 1.1. Przedmiot

Odpowiedzialność i rozliczalność stanowią dwie strony tego samego medalu i są istotnymi składnikami dobrego zarządzania. Dostateczne zaufanie można rozwinąć jedynie, gdy wykaże się, że odpowiedzialność skutecznie funkcjonuje w praktyce. Utrzymanie bezpieczeństwa danych osobowych, minimalizowanie ryzyka, budowanie i podtrzymywanie dobrej opinii, oraz dbałość o zaufanie klientów są decydujące dla Szpitala Specjalistyczny w Prabutach Sp. z o.o. w tym celu stosuje się rzeczywiste środki ochrony danych mające na celu zapewnienie dobrego zarządzania w zakresie ochrony danych, przy jednoczesnym minimalizowaniu ryzyka prawnego i gospodarczego, a także ryzyka naruszenia dobrej opinii, mogących wynikać z niewłaściwych praktyk w zakresie ochrony danych.

Utrzymanie bezpieczeństwa przetwarzanych przez Szpital Specjalistyczny w Prabutach Sp. z o.o. danych osobowych rozumiane jest jako zapewnienie ich poufności, integralności i dostępności, rozliczalności na odpowiednim poziomie, a także odporności systemów informatycznych. Miarą bezpieczeństwa jest wielkość ryzyka związanego z zasobem stanowiącym przedmiot niniejszej Polityki.



Przedmiotem Polityki Ochrony Danych są zasady i tryb postępowania z danymi osobowymi uznanymi przez Szpital Specjalistyczny w Prabutach Sp. z o.o..

Polityka Ochrony Danych dotyczy zarówno danych osobowych i informacji przetwarzanych w Szpital Specjalistyczny w Prabutach Sp. z o.o. w systemach informatycznych, jak i w sposób tradycyjny, z wykorzystaniem nośników papierowych.

Zasady określone w Polityce Ochrony Danych mają zastosowanie do wszystkich osób upoważnionych przez Administratora Danych do przetwarzania danych osobowych.

Niniejsza procedura została opracowana na podstawie:


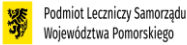
- Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych) – dalej „*Rozporządzenie PE*”,
- Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych – dalej „*Ustawa*”,
- Innych dokumentów pomocniczych w sprawie systemu ochrony danych osobowych m.in. Wytycznych i Opiniach Grupy Roboczej ds. Ochrony Danych.

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	PROCEDURA	Wydanie: 3	10.08.2025
			Strona 5 z 81
	POLITYKA OCHRONY DANYCH OSOBOWYCH	Nr dokumentu: <b>7- Pr5</b>	

## 1.2. Terminologia i określenia

W niniejszej Polityce Danych Osobowych obowiązuje terminologia i określenia zawarte w Rozporządzeniu PE. Ponadto ilekroć w Polityce Ochronie Danych jest mowa o:

- **POD** – należy przez to rozumieć dokument Polityki Ochrony Danych,
- **Administratorze Danych (ADO)** – należy przez to rozumieć Szpital Specjalistyczny w Prabutach Sp. z o.o. reprezentowana przez Zarząd,
- **IOD** - należy przez to rozumieć Inspektora Ochrony Danych,
- **ASI** - należy przez to rozumieć Administratora Systemów Informatycznych
- **Stronie trzeciej** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe,
- **Użytkownika** - należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w Szpital Specjalistyczny w Prabutach Sp. z o.o.. Użytkownikiem może być etatowy pracownik, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilnoprawnej, czy kontraktu,
- **przetwarzaniu** – należy przez to rozumieć operację lub zestaw operacji na danych, takich jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,
- **sieci lokalnej** - system umożliwiający bezpośrednią komunikację wielu niezależnych urządzeń rozmieszczonych na stosunkowo niewielkim obszarze za pośrednictwem fizycznych kanałów komunikacyjnych wyłącznie dla potrzeb Szpital Specjalistyczny w Prabutach Sp. z o.o.,
- **sieci rozległej** - należy przez to rozumieć publiczną sieć telekomunikacyjną w rozumieniu ustawy z dnia z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne i nie będącą siecią lokalną,
- **Rozporządzeniu PE** – należy przez to rozumieć Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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 osobowych),
- **Ustawie** – należy przez to rozumieć ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych,
- **Organ nadzorczy** - należy przez to rozumieć Prezesa Urzędu Ochrony Danych Osobowych zgodnie z Ustawą o Ochronie danych osobowych z dnia 10 maja 2018 r.,
- **poufności informacji** – należy przez to rozumieć zapewnienie, że tylko uprawnieni pracownicy mają dostęp do informacji,
- **integralności informacji** – należy przez to rozumieć zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania,

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	PROCEDURA	Wydanie: 3	10.08.2025
		Strona 6 z 81	
	POLITYKA OCHRONY DANYCH OSOBOWYCH	Nr dokumentu: <b>7- Pr5</b>	

- **dostępności informacji** – należy przez to rozumieć zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,
- **ryzyku** – należy przez to rozumieć wpływ niepewności na cele. Ryzyko w bezpieczeństwie informacji to potencjalna sytuacja, gdzie określone zdarzenie wykorzysta podatność (słabość) aktywów powodując szkodę w organizacji,
- **zarządzaniu ryzykiem** – należy przez to rozumieć proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa przetwarzanych danych osobowych,
- **naruszeniu bezpieczeństwa** – należy przez to rozumieć 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,
- **incydencie bezpieczeństwa** – należy przez to rozumieć zdarzenie potencjalnie naruszającego bezpieczeństwo danych/informacji,


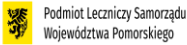
Dodatkowo zarządzanie bezpieczeństwem danych osobowych wiąże się z zapewnieniem:

- **rozliczalności działań** – rozumianej jako zapewnienie, że wszystkie działania istotne dla przetwarzania danych osobowych zostały zarejestrowane w systemie i możliwym jest zidentyfikowanie użytkownika, który działania wykonał.  
Rozliczalność oznacza wdrożenie środków (w tym wewnętrznych procedur) gwarantujących przestrzeganie przepisów o ochronie danych w związku z operacjami ich przetwarzania oraz sporządzenie dokumentacji wskazującej osobom, których dane dotyczą, oraz organom nadzorczym, jakie środki podjęto, aby zapewnić przestrzeganie przepisów o ochronie danych osobowych.

### 1.3. Cel i strategię bezpieczeństwa

Wdrożenie w Szpitalu Specjalistycznym w Prabutach Sp. z o.o. Polityki Ochrony Danych ma na celu zabezpieczenie przetwarzanych przez Szpital Specjalistyczny w Prabutach Sp. z o.o. danych osobowych przetwarzanych w systemie tradycyjnym i w systemach informatycznych poprzez wykonanie obowiązków wynikających z Rozporządzenia PE, Ustawy o ochronie danych osobowych i przepisów wykonawczych. Ponieważ system informatyczny Szpitalu Specjalistycznym w Prabutach Sp. z o.o., służący do przetwarzania danych osobowych posiada również połączenie z Internetem, niniejsza Polityka Ochrony Danych służy zapewnieniu środków bezpieczeństwa **na poziomie wysokim**. Polityka Ochrony Danych opisuje zabezpieczenia organizacyjne i techniczne chroniące przed nieuprawnionym dostępem, zawierając tym samym zbiór zasad dotyczących przetwarzania danych osobowych i ich zabezpieczenia.

*Cele Szpitala Specjalistycznego w Prabutach Sp. z o.o. w zakresie bezpieczeństwa danych osobowych:*

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	PROCEDURA	Wydanie: 3	<b>10.08.2025</b>
			Strona 7 z 81
	POLITYKA OCHRONY DANYCH OSOBOWYCH	Nr dokumentu: <b>7- Pr5</b>	

- zapobieganie naruszeń bezpieczeństwa w systemie ochrony danych osobowych,
- zapewnienie zgodności z prawem podejmowanych działań,
- ochrona wizerunku, uzyskanie i utrzymanie odpowiednio wysokiego poziomu bezpieczeństwa danych osobowych przetwarzanych przez Szpital Specjalistyczny w Prabutach Sp. z o.o., rozumiane jako zapewnienie poufności, integralności, zapewnienie rozliczalności podejmowanych działań oraz odporności systemów informatycznych.

*Cele osiągnięte są przez realizowane strategie:*

- zapewnienie wsparcia zarządzających dla zadania ochrony danych osobowych,
- właściwą organizację ochrony danych osobowych, w tym przygotowanie dokumentacji w sposób umożliwiający wykazanie rozliczalności w zakresie ochrony danych osobowych,
- zarządzanie ryzykiem w ochronie danych osobowych w celu ograniczenia go do akceptowanego poziomu.


#### 1.4. Zasady dotyczące przetwarzania danych osobowych [5]

**Dane osobowe muszą być przetwarzane:**

- przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („**zgodność z prawem, rzetelność i przejrzystość**”);
- zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami („**ograniczenie celu**”);
- adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („**minimalizacja danych**”);
- 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**”);
- 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 („**ograniczenie przechowywania**”);
- 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**”).


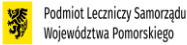
#### 1.5. Zgodność przetwarzania z prawem [6]

- Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:
  - osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
  - 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. Termin „niezbędne do wykonania umowy” musi być interpretowany ściśle.

<p>Szpital Specjalistyczny w Prabutach sp. z o.o.</p>  <p>Podmiot Leczniczy Samorządu Województwa Pomorskiego</p>	<p>PROCEDURA</p>	Wydanie: 3	10.08.2025
		Strona 8 z 81	
	<p>POLITYKA OCHRONY DANYCH OSOBOWYCH</p>	Nr dokumentu: <b>7- Pr5</b>	

Przetwarzanie musi być niezbędne do wypełnienia umowy z każdą indywidualną osobą, której dane dotyczą. W kontekście zatrudnienia ta podstawa może pozwolić na przykład na przetwarzanie informacji dotyczących płac i rachunku bankowego, tak aby można było wypłacić wynagrodzenia. Musi istnieć bezpośrednie i obiektywne powiązanie między przetwarzaniem danych i celem wykonania umowy. Konieczność wykonania umowy nie może być podstawą prawną przetwarzania szczególnych kategorii danych;

- c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na ADO. Podstawa przetwarzania musi być określona w prawie Unii lub w prawie państwa członkowskiego, któremu podlega ADO, a cel przetwarzania musi być określony w tej podstawie prawnej;
  - d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
  - e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej ADO. Podstawa przetwarzania musi być określona w prawie Unii lub w prawie państwa członkowskiego, któremu podlega ADO, a cel przetwarzania musi być określony w tej podstawie prawnej lub, musi być ono niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej ADO;
  - f) 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.
- 2) Artykuł 6 Rozporządzenia PE ustala warunki legalnego przetwarzania danych osobowych i opisuje sześć legalnych przesłanek, na których ADO może polegać. Zastosowanie jednego z tych sześciu warunków musi zostać ustalone przed przetwarzaniem i w odniesieniu do określonego celu. Co do zasady przetwarzanie dla jednego konkretnego celu nie może opierać się na wielu legalnych podstawach. Niemniej jednak można polegać na więcej niż jednej przesłance do legalizacji przetwarzania, w przypadku gdy dane są wykorzystywane do różnych celów, a każdy cel musi być połączony z którąś z podstaw. Jednak to ADO musi z wyprzedzeniem zidentyfikować cele i ich odpowiednie, zgodne z prawem podstawy przetwarzania danych. Podstawa nie może być modyfikowana w toku przetwarzania. W związku z tym ADO nie może dokonywać zmian między przesłankami. Na przykład nie będzie możliwe retroaktywne zastosowanie przesłanki uzasadnionego interesu, w sytuacji powstania wątpliwości co do ważności zgody. Dlatego ADO w przypadku, gdy uzyskuje zgodę na przetwarzanie danych osobowych, zasadniczo nie polega na innych legalnych podstawach określonych w art. 6 Rozporządzenia PE jako "zapasowych", jeżeli nie jest on w stanie wykazać, że osoba, której dane dotyczą, udzieliła zgody spełniającej warunki z Rozporządzenia PE lub jeśli nastąpiło jej wycofanie. Ze względu na obowiązek wykazania

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	PROCEDURA	Wydanie: 3	10.08.2025
			Strona 9 z 81
	POLITYKA OCHRONY DANYCH OSOBOWYCH	Nr dokumentu: <b>7- Pr5</b>	



podstawy przetwarzania danych, na której opiera się ADO w momencie zbierania danych, istotne jest uprzednie zdecydowanie, która podstawa będzie najwłaściwsza.

- 3) 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 lub prawa państwa członkowskiego, ADO – aby ustalić, czy przetwarzanie w innym celu jest zgodne z celem, w którym dane osobowe zostały pierwotnie zebrane – bierze pod uwagę między innymi:
  - a) wszelkie związki między celami, w których zebrano dane osobowe, a celami zamierzonego dalszego przetwarzania;
  - b) kontekst, w którym zebrano dane osobowe, w szczególności relację między osobami, których dane dotyczą, a ADO;
  - c) charakter danych osobowych, w szczególności czy przetwarzane są szczególne kategorie danych osobowych zgodnie z art. 9 Rozporządzenia PE lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa zgodnie z art. 10 Rozporządzenia PE;
  - d) ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą;
  - e) istnienie odpowiednich zabezpieczeń, w tym ewentualnie szyfrowania lub pseudonimizacji.
- 4) ADO w nawiązaniu do powyższego punktu przygotowuje Opinię dotyczącą ustalenia, czy przetwarzanie w innym celu jest zgodne z celem, w którym dane osobowe zostały pierwotnie zebrane.
- 5) Jeżeli ADO zamierza przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały pierwotnie zebrane, wówczas ADO po określeniu nowych celów i wyznaczeniu dla nich podstawy prawnej przetwarzania, informuje osobę, której dane dotyczą zgodnie z pkt. 3.1.3 POD lub jeżeli dane mają być przetwarzane na podstawie zgody ADO działa zgodnie z pkt. 3.1.4 POD.



## 1.6. Przetwarzanie szczególnych kategorii danych osobowych [9]

Przetwarzanie danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby, jest zgodne z prawem wyłącznie w przypadkach, gdy spełniony jest jeden z poniższych warunków:

- a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu przetwarzania szczególnych kategorii danych osobowych, o którym mowa w art. 9 ust. 1 Rozporządzenia PE;

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Lecznicy Samorządu Województwa Pomorskiego	PROCEDURA	Wydanie: 3	<b>10.08.2025</b>
			Strona 10 z 81
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

- b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez ADO lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;
- c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
- d) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem, że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz, że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;
- e) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
- f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
- g) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;
- h) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem następujących warunków i zabezpieczeń: jeżeli są przetwarzane przez – lub na odpowiedzialność – pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe lub przez inną osobę również podlegającą obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe;
- i) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie


 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
			Strona 11 z 81
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;



- j) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 Rozporządzenia PE, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

### **1.7. Przetwarzanie danych osobowych w miejscu pracy**

- 1) Przy przetwarzaniu danych osobowych pracowników ADO pamięta o podstawowych zasadach ochrony danych, niezależnie od stosowanej technologii.
- 2) ADO wdraża odpowiednie i szczegółowe środki zapewniające pracownikom poszanowanie ich godności, prawnie uzasadnionych interesów i praw podstawowych.
- 3) Treść komunikacji elektronicznej wychodzącej z lokalu przedsiębiorstwa jest objęta taką samą ochroną praw podstawowych co komunikacja analogowa.
- 4) Międzynarodowe przekazywanie danych pracowników powinno się odbywać tylko wówczas, gdy zapewniony jest odpowiedni stopień ochrony.
- 5) ADO zapewnia, aby dane, które są proporcjonalne i niezbędne, przetwarzano do określonych i prawnie uzasadnionych celów.
- 6) ADO uwzględnia zasadę ograniczenia celu, upewniając się jednocześnie, że dane są prawidłowe, stosowne oraz nienadmierne ilościowo w stosunku do prawnie uzasadnionego celu.
- 7) ADO stosuje zasadę proporcjonalności i pomocniczości niezależnie od obowiązującej podstawy prawnej.
- 8) ADO umożliwia osobom, których dane dotyczą, korzystanie z przysługujących im praw, w tym prawa dostępu i, w stosownych przypadkach, prawa do sprostowania, usunięcia lub zablokowania danych osobowych.
- 9) ADO aktualizuje dane i nie przechowuje ich dłużej niż to konieczne.
- 10) ADO stosuje wszystkie środki konieczne do ochrony danych przed nieuprawnionym wykorzystaniem i zapewnia, aby pracownicy byli wystarczająco świadomi obowiązków ochrony danych.
- 11) ADO przed wdrożeniem jakiegokolwiek narzędzia monitorowania przeprowadza analizę proporcjonalności, aby zbadać, czy wszystkie dane są niezbędne, czy konieczność przetwarzania danych przeważa nad ogólnymi prawami pracowników do prywatności, które przysługują im również w miejscu pracy, oraz czy w danym przypadku zachodzi potrzeba wdrożenia środków zapewniających ograniczenie skali naruszenia prawa do życia i poufności komunikacji do niezbędnego minimum.


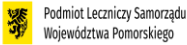
Szpital Specjalistyczny w Prabutach sp. z o.o.   Podmiot Leczniczy Samorządu Województwa Pomorskiego	PROCEDURA	Wydanie: 3	10.08.2025
		Strona 12 z 81	
	POLITYKA OCHRONY DANYCH OSOBOWYCH	Nr dokumentu: <b>7- Pr5</b>	

- 12) ADO zapewnia żeby operacje przetwarzania były zgodne z wymogami przejrzystości i skutecznie informuje pracowników o wszelkich środkach monitorowania wdrożonych w miejscu pracy, celach tego monitorowania oraz okolicznościach, w których się ono odbywa, a także działaniach, które pracownicy mogą podejmować, aby uniemożliwić gromadzenie ich danych przez technologie monitorowania. ADO zapewnia, by Polityka i zasady dotyczące zgodnego z prawem monitorowania były przejrzyste i łatwo dostępne i w miarę możliwości włącza reprezentatywną grupę pracowników w proces opracowywania i oceny takich zasad i polityki, ponieważ większość działań w obszarze monitorowania może wiązać się z ingerencją w życie prywatne pracowników.
- 13) Przy przetwarzaniu danych osobowych pracowników ADO bierze pod uwagę następujące kwestie:
- W odniesieniu do większości przypadków przetwarzania danych w miejscu pracy podstawą prawną nie może i nie powinna być zgoda pracowników (art. 6 lit. a Rozporządzenia PE)) ze względu na charakter stosunków między pracodawcą a pracownikiem. Pracownicy rzadko mogą dobrowolnie udzielić zgody, odmówić zgody lub cofnąć zgodę, z uwagi na zależność wynikającą ze stosunku pracy między pracodawcą a pracownikiem. Poza wyjątkowymi sytuacjami przy przetwarzaniu danych osobowych pracowników ADO polega na innej podstawie prawnej niż zgoda. Ponadto nawet w przypadkach, w których zgodę można uznać za ważną podstawę prawną takiego przetwarzania (tj. jeżeli można bez wątpienia stwierdzić, że zgoda jest dobrowolna), musi ona stanowić konkretne i świadome wskazanie przez pracownika. Domyślne ustawienia urządzeń lub zainstalowanie oprogramowania, które ułatwia elektroniczne przetwarzanie danych osobowych, nie może kwalifikować się jako zgoda wyrażona przez pracowników, ponieważ zgoda wymaga aktywnego oświadczenia woli.
  - Przetwarzanie może być konieczne do realizacji umowy (art. 6 lit. b Rozporządzenia PE), w przypadkach gdy pracodawca musi przetwarzać dane osobowe pracownika w celu wywiązania się z takich zobowiązań. Stosunki pracy często opierają się na umowie o pracę zawartej między pracodawcą a pracownikiem. Przy wypełnianiu obowiązków wynikających z tej umowy, takich jak wypłacanie pracownikowi wynagrodzenia, pracodawca jest zobowiązany do przetworzenia pewnych danych osobowych.
  - Często zdarza się, że prawo pracy może nakładać obowiązki prawne (art. 6 lit. c Rozporządzenia PE)), które wymagają przetwarzania danych osobowych (np. do celów obliczenia wysokości podatku i zarządzania wynagrodzeniami). Wówczas prawo takie stanowi podstawę prawną przetwarzania danych. W takich przypadkach należy wyraźnie i w sposób wyczerpujący poinformować pracownika o takim przetwarzaniu (chyba, że ma zastosowanie wyjątek).
  - Jeżeli pracodawca próbuje powoływać się na uzasadniony interes (art. 6 lit. f Rozporządzenia PE)), cel przetwarzania danych musi być zgodny z prawem. Wybrana metoda lub określona technologia musi być konieczna z punktu widzenia uzasadnionego interesu pracodawcy, proporcjonalna i wdrażana w możliwie najmniej inwazyjny

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Lecznicy Samorządu Województwa Pomorskiego	PROCEDURA	Wydanie: 3	<b>10.08.2025</b>
			Strona 13 z 81
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

sposób, a także musi umożliwiać pracodawcy wykazanie, że wprowadzono odpowiednie środki w celu zapewnienia równowagi z podstawowymi prawami i wolnościami pracowników. Przetwarzanie danych musi być również proporcjonalne do potrzeb biznesowych, tj. celu, który ma zostać osiągnięty. Przetwarzanie danych w miejscu pracy należy prowadzić w sposób jak najmniej inwazyjny i tak, by było ukierunkowane na konkretny obszar ryzyka. Ponadto, jeżeli pracodawca powołuje się na art. 6 lit. f) Rozporządzenia PE, pracownik zachowuje prawo sprzeciwu wobec przetwarzania z ważnych i uzasadnionych przyczyn zgodnie z art. 21 Rozporządzenia PE. Prawnie uzasadniony interes sam w sobie nie wystarcza, aby przetwarzanie było nadrzędne wobec praw i wolności pracowników. Niezależnie od podstawy prawnej takiego przetwarzania przed jego rozpoczęciem ADO przeprowadza analizę proporcjonalności, aby ustalić, czy przetwarzanie jest konieczne do osiągnięcia prawnie uzasadnionego celu, oraz rozważa środki, jakie należy wdrożyć, aby zapewnić ograniczenie naruszeń praw do życia prywatnego i tajemnicy komunikacji do minimum. Może to stanowić część oceny skutków dla ochrony danych.

- 14) Przy przetwarzaniu danych osobowych pracowników niekiedy ADO może powołać się na wykonanie umowy i prawnie uzasadnione interesy, pod warunkiem że przetwarzanie danych jest bezwzględnie konieczne ze względów prawnych i zgodne z zasadą proporcjonalności i pomocniczości.
- 15) Treść art. 22 Rozporządzenia PE o ochronie danych przyznaje osobom, których dane dotyczą, prawo do nieobjęcia ich decyzją opartą wyłącznie na zautomatyzowanym przetwarzaniu, w przypadku gdy taka decyzja wywołuje skutki prawne, które ich dotyczą lub mają na nie istotny wpływ, oraz oparta jest wyłącznie na zautomatyzowanym przetwarzaniu danych, którego celem jest dokonanie oceny niektórych dotyczących ich aspektów o charakterze osobistym, jak np. wyniki osiągane w pracy, chyba że decyzja jest konieczna w celu zawarcia lub realizacji umowy, jest dozwolona przez prawo UE lub prawo państw członkowskich bądź opiera się na wyraźnej zgodzie osoby, której dane dotyczą.
- 16) Art. 25 Rozporządzenia PE wymaga, aby administratorzy danych uwzględniali ochronę danych w fazie projektowania oraz domyślną ochronę danych. Na przykład: w przypadku gdy pracodawca wydaje pracownikom urządzenia, należy wybrać rozwiązania najbardziej sprzyjające zachowaniu prywatności, jeżeli wykorzystywane są technologie śledzące. Należy również wziąć pod uwagę minimalizację danych.
- 17) W art. 35 Rozporządzenia PE określono wymogi dotyczące prowadzenia oceny skutków dla ochrony danych przez administratora danych, jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele przetwarzania z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Przykładem jest systematyczna, kompleksowa ocena 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

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	PROCEDURA	Wydanie: 3	<b>10.08.2025</b>
			Strona 14 z 81
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	



znacząco wpływających na osobę fizyczną. Jeżeli w ocenie skutków dla ochrony danych zostanie wykazane, że administrator danych nie jest w stanie w wystarczającym stopniu wyeliminować zidentyfikowanego ryzyka, tj. ryzyko szczątkowe pozostaje wysokie, wówczas przed rozpoczęciem przetwarzania administrator danych musi skonsultować się z organem nadzorczym (art. 36 ust. 1 Rozporządzenia PE).

18) Operacja przetwarzania w trakcie procesu rekrutacji:

- a) ADO gromadzi i przetwarza dane osobowe osób ubiegających się o pracę w takim zakresie, w jakim gromadzenie tych danych jest konieczne i istotne dla wykonywania pracy, o którą się ubiegają.
- b) ADO właściwie informuje daną osobę o przetwarzaniu do celów rekrutacji zanim weźmie ona udział w procesie rekrutacji.
- c) W przypadkach, gdy ADO zechce zatrzymać dane na wypadek wystąpienia kolejnej możliwości zatrudnienia, osoba, której dane dotyczą, zostaje odpowiednio poinformowana i ma możliwość wyrażenia zgody na dalszą rekrutację i przetwarzanie danych.
- d) ADO może wskazać podstawę prawną na mocy art. 6 lit. f) Rozporządzenia PE do przeprowadzenia przeglądu publicznie dostępnych informacji o kandydatach, jedynie w przypadku gdy na potrzeby zatrudnienia konieczne jest dokonanie przeglądu informacji o kandydacie znajdujących się w mediach społecznościowych, np. aby móc ocenić konkretne zagrożenia związane z kandydatami na dane stanowisko, a kandydaci zostaną odpowiednio poinformowani (np. w tekście ogłoszenia o pracę).


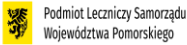
19) Operacje przetwarzania wynikające z badania przeprowadzonego pod kątem zatrudnienia:

- a) Badanie profili pracowników w mediach społecznościowych nie powinno stanowić ogólnej praktyki, ponieważ monitorowanie pracowników poprzez gromadzenie informacji na temat ich znajomych, opinii, przekonań, zainteresowań, zwyczajów, miejsc pobytu, postaw i zachowań, jest pozyskiwaniem danych, w tym danych wrażliwych, na temat życia prywatnego i rodzinnego pracownika.
- b) Dopóki ADO może udowodnić, że takie monitorowanie jest konieczne do ochrony jego uzasadnionych interesów, nie ma innych, mniej inwazyjnych środków oraz że pracownicy zostali odpowiednio poinformowani o zakresie regularnego obserwowania ich publicznych informacji, wówczas może powołać się na podstawę prawną w postaci art. 6 lit. f) Rozporządzenia PE.
- c) ADO nie wymaga od pracownika lub osoby ubiegającej się o zatrudnienie dostępu do informacji, którymi dzieli się ona z innymi osobami za pośrednictwem sieci społecznościowych.
- d) ADO zapewnia, aby pracownicy nie powinni być zobowiązani do korzystania z profili w mediach społecznościowych zapewnianych przez ich pracodawcę. Nawet jeżeli jest to wyraźnie przewidziane w świetle ich zadań, ADO zapewnia, aby umowa o pracę zawierała warunki gwarantujące pracownikowi prawo do zachowania niepublicznego

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Lecznicy Samorządu Województwa Pomorskiego	PROCEDURA	Wydanie: 3	<b>10.08.2025</b>
		Strona 15 z 81	
	POLITYKA OCHRONY DANYCH OSOBOWYCH	Nr dokumentu: <b>7- Pr5</b>	


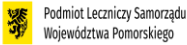
profilu „niezwiązanego z pracą”, z którego mogą korzystać zamiast „oficjalnego” profilu związanego z pracodawcą.

- 20) Operacje przetwarzania wynikające z monitorowania korzystania z ICT w miejscu pracy:
- ADO zdaje sobie sprawę, że głównym zagrożeniem dla prywatności pracowników jest monitorowanie treści komunikacji elektronicznej w miejscu pracy (np. połączeń telefonicznych, przeglądanych zasobów internetowych, wiadomości e-mail, komunikatów natychmiastowych, połączeń za pośrednictwem telefonii internetowej itd.).
  - ADO poświęca znacznie większą wagę działaniom prewencyjnym niż działaniom mającym na celu wykrycie określonych zachowań, bowiem interesy pracodawcy można chronić skuteczniej, zapobiegając niewłaściwemu korzystaniu z internetu, niż przeznaczając dodatkowe zasoby na wykrywanie nadużyć. Monitorowanie całej aktywności pracowników w internecie stanowi nieproporcjonalną reakcję naruszającą prawo do poufności komunikacji.
  - Jeżeli w niektórych przypadkach przechwytywanie danych przekazywanych za pośrednictwem protokołu TLS może okazać się bezwzględnie konieczne, wówczas ADO zapewnia, by urządzenie zostało skonfigurowane w taki sposób, aby uniemożliwić ciągłe rejestrowanie działalności pracownika, na przykład poprzez blokowanie podejrzanych danych przychodzących lub wychodzących i przekierowywanie użytkownika do portalu informacyjnego, z poziomu którego może on zwrócić się o dokonanie przeglądu takiej zautomatyzowanej decyzji. Jeżeli mimo to zachodziłaby bezwzględna konieczność zastosowania pewnej formy ogólnego rejestrowania, urządzenie można skonfigurować również w taki sposób, aby nie gromadziło danych dziennika, jeżeli urządzenie nie zasygnalizowało wystąpienia określonego zdarzenia, co pozwala ograniczyć gromadzone informacje do minimum.
  - ADO określa, jeżeli jest to wymagane, kiedy można uzyskać dostęp do podejrzanych danych dziennika i kto jest uprawniony do uzyskania takiego dostępu, oraz w przystępny i trwały sposób udostępnia ją wszystkim pracownikom jako dodatkowe wytyczne w kwestii dozwolonych i niedozwolonych sposobów korzystania z sieci i urządzeń. Co pozwoli pracownikom tak zmodyfikować swoje zachowanie, aby uniknąć bycia monitorowanym w trakcie uprawnionego korzystania z aplikacji IT w miejscu pracy do celów prywatnych.
  - Niezależnie od danej technologii lub oferowanych przez nią funkcji, na podstawie prawnej w postaci art. 6 lit. f) Rozporządzenia PE ADO może powołać się wyłącznie wówczas, gdy przetwarzanie danych spełnia określone warunki: (1) korzystając z tego rodzaju produktów lub aplikacji bierze pod uwagę proporcjonalność wdrażanych przez siebie środków, a także to, czy w danej sytuacji można podjąć jakiegokolwiek dodatkowe działania, aby ograniczyć lub zmniejszyć skalę i skutki przetwarzania danych (przed wprowadzeniem jakiegokolwiek technologii monitorowania ADO przeprowadza tego rodzaju analizę w ramach oceny skutków dla ochrony danych) (2). Reprezentatywna

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	PROCEDURA	Wydanie: 3	<b>10.08.2025</b>
			Strona 16 z 81
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	


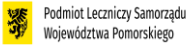
próba pracowników każdorazowo powinna uczestniczyć w ocenie konieczności monitorowania, a także logiki polityki i jej dostępności.

- f) Aby ADO mógł powołać się na swój uzasadniony interes, powinny zostać wdrożone określone środki ograniczające ryzyko. Na przykład zasady stosowane przez system przy ustalaniu, czy daną wiadomość e-mail można uznać za stwarzającą ryzyko potencjalnego naruszenia ochrony danych, powinny być w pełni przejrzyste dla użytkowników, a w przypadku gdy system uzna, że wysyłana wiadomość email może doprowadzić do naruszenia ochrony danych, nadawca tej wiadomości e-mail powinien zostać powiadomiony o tym fakcie za pomocą komunikatu ostrzegawczego przed wysłaniem wiadomości, aby umożliwić mu rezygnację z jej wysłania.
- g) W niektórych przypadkach pracowników można monitorować nie poprzez wdrażanie określonych technologii, ale z uwagi na fakt, że korzystają oni z aplikacji internetowych udostępnionych im przez ADO, które przetwarzają dane osobowe. Na przykład aplikacje biurowe bazujące na technologii przetwarzania w chmurze (np. edytory dokumentów, kalendarze, portale społecznościowe). Wówczas ADO zapewnia pracownikom możliwość wyznaczenia określonych przestrzeni prywatnych, do których ADO będzie mógł uzyskać dostęp wyłącznie w wyjątkowych okolicznościach. Ma to znaczenie na przykład w przypadku kalendarzy, które często są wykorzystywane również do planowania prywatnych spotkań. Jeżeli pracownik określi dane spotkanie jako „Prywatne” lub zawrze odpowiednią uwagę w samym opisie spotkania, wówczas ADO (i inni pracownicy) nie powinni mieć możliwości zapoznania się z opisem spotkania.
- 21) Operacje przetwarzania wynikające z monitorowania korzystania z ICT poza miejscem pracy:
- a) Monitorowanie pracy w domu i pracy zdalnej - w takiej sytuacji pracodawca udostępnia pracownikowi sprzęt ICT lub oprogramowanie, które – po jego zainstalowaniu w domu pracownika lub na należących do niego urządzeniach – pozwala mu uzyskać taki sam poziom dostępu do sieci, systemów i zasobów pracodawcy, jakim dysponowałby wówczas, gdyby znajdował się w miejscu pracy, w zależności od stopnia wdrożenia odpowiednich rozwiązań. W takim przypadku ADO wdraża odpowiednie środki techniczne, aby ryzyko uzyskania nieuprawnionego dostępu do danych nie wzrosło i nie doprowadziło do utraty lub zniszczenia informacji znajdujących się w posiadaniu ADO, w tym danych osobowych pracowników lub konsumentów. Kluczowe znaczenie ma ograniczenia ryzyka związanego z pracą z domu lub pracą zdalną w proporcjonalny, adekwatny sposób, niezależnie od formy wykonywania takiej pracy i od wykorzystywanej w tym celu technologii, w szczególności w przypadku, gdy granica między korzystaniem z danego urządzenia w celach związanych z pracą i w celach prywatnych jest płynna.
- b) Korzystanie z własnego sprzętu – taki sposób wykonywania pracy z definicji wiąże się z tym, że część operacji wykonywanych przez pracownika na danym urządzeniu będzie

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Lecznicy Samorządu Województwa Pomorskiego	PROCEDURA	Wydanie: 3	10.08.2025
			Strona 17 z 81
	POLITYKA OCHRONY DANYCH OSOBOWYCH	Nr dokumentu: <b>7- Pr5</b>	

miała osobisty charakter, dlatego też ADO nie zezwala na korzystanie z własnego sprzętu do celów firmowych.

- c) Zarządzanie urządzeniami mobilnymi umożliwia pracodawcom zdalne lokalizowanie urządzeń, wdrażanie określonych ustawień lub aplikacji oraz usuwanie danych na żądanie. Pracodawca może obsługiwać tę funkcję samodzielnie lub zlecić to zadanie osobie trzeciej. Usługi zarządzania urządzeniami mobilnymi umożliwiają również pracodawcom rejestrowanie lub śledzenie urządzenia w czasie rzeczywistym, nawet jeżeli nie zgłoszono jego kradzieży. W związku z powyższym ADO przed wprowadzeniem jakiegokolwiek technologii tego rodzaju, przeprowadza Ocenę skutków dla ochrony danych. Jeżeli ocena skutków dla ochrony danych wykáže, że wdrożenie technologii zarządzania urządzeniami mobilnymi jest konieczne w danych okolicznościach, ADO nadal przeprowadza ocenę w celu ustalenia, czy przetwarzanie danych wynikające z zastosowania tej technologii jest zgodne z zasadami proporcjonalności i pomocniczości, celem zagwarantowania, że dane gromadzone przy wykorzystaniu wspomnianej funkcji zdalnego określania lokalizacji będą przetwarzane w określonym celu oraz że nie będą stanowiły i nie będą mogły stanowić elementu szerszej zakrojonego programu ciągłego monitorowania pracowników. Funkcje śledzenia należy ograniczyć, nawet gdy korzysta się z nich w określonych celach. Systemy śledzenia mogą zostać zaprojektowane w taki sposób, by umożliwiały rejestrowanie danych o lokalizacji bez przedstawiania ich pracodawcy – w takiej sytuacji dane o lokalizacji powinny zostać udostępnione pracodawcy wyłącznie w przypadku zgłoszenia urządzenia lub jego utraty. ADO zapewnia, aby pracownicy, których urządzenia są objęte usługami zarządzania urządzeniami mobilnymi, uzyskali wyczerpujące informacje na temat tego, jakie środki śledzenia są stosowane i jakie to ma dla nich konsekwencje.
- d) Operacje przetwarzania związane z czasem pracy i obecnością w miejscu pracy - systemy zapewniające pracodawcom możliwość kontrolowania osób uprawnionych do wejścia na teren ich lokalu lub uzyskania dostępu do określonych obszarów w takim lokalu mogą zapewniać również możliwość śledzenia działań pracowników. Niektóre z tych technologii wiążą się z przetwarzaniem danych biometrycznych, podczas gdy inne umożliwiają śledzenie urządzeń mobilnych. Ze względu na ryzyko polegające na zapewnianiu inwazyjnego poziomu wiedzy na temat działań podejmowanych przez pracownika w miejscu pracy i kontroli nad tymi działaniami, ADO nie stosuje w/w systemów.
- e) Operacje przetwarzania związane z pojazdami, z których korzystają pracownicy - ADO nie posiada pojazdów firmowych.
- f) Rejestratory danych na temat zdarzeń - ADO nie posiada pojazdów firmowych i nie korzysta z rejestratorów danych na temat zdarzeń.
- g) Operacje przetwarzania wiążące się z międzynarodowym przekazywaniem danych kadrowych oraz innych danych dotyczących pracowników – korzystanie z większości aplikacji i usług w chmurze, takich jak aplikacje i usługi służące do przetwarzania

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Lecznicy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
		Strona 18 z 81	
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

danych kadrowych oraz internetowe aplikacje biurowe skutkuje międzynarodowym przekazywaniem danych pracowników, a przekazywanie danych osobowych państwu trzeciemu spoza UE można uznać za dopuszczalne wyłącznie w przypadku, gdy państwo to zapewnia odpowiedni stopień ochrony. Niezależnie od podstawy prawnej, przekazywanie danych musi odbywać się zgodnie z przepisami Rozporządzenia PE. Dlatego też należy zapewnić zgodność ze stosownymi przepisami dotyczącymi międzynarodowego przekazywania danych.



- 22) Fakt, że pracodawca jest właścicielem środków elektronicznych, nie znosi prawa pracowników do poufności komunikacji związanej z danymi o lokalizacji i korespondencją. W związku z czym śledzenie lokalizacji pracowników za pomocą ich własnych urządzeń lub urządzeń firmowych ADO ogranicza do sytuacji, w których takie śledzenie jest bezwzględnie konieczne do osiągnięcia uzasadnionego celu.
- 23) ADO zdaje sobie sprawę, że wprowadzenie całkowitego zakazu komunikowania w celach prywatnych jest niepraktyczne, a egzekwowanie przestrzegania tego zakazu może wymagać wdrożenia nieproporcjonalnego poziomu monitorowania. Dlatego działaniom prewencyjnym przypisuje znacznie większą wagę niż działaniom mającym na celu wykrycie określonych zachowań. Technologie monitorowania komunikacji mogą mieć również negatywny wpływ na prawa podstawowe pracowników do organizowania się, organizowania spotkań pracowniczych oraz do komunikowania się w sposób poufny (w tym na prawo do uzyskiwania informacji). Szerokie wykorzystanie technologii monitorowania może również zmniejszyć gotowość (i liczbę kanałów służących do tego celu) pracowników do informowania pracodawców o nieprawidłowościach lub nielegalnych działaniach przełożonych lub innych pracowników, które mogą zaszkodzić działalności (zwłaszcza danym klientów) lub miejscu pracy. Często konieczne jest zapewnienie anonimowości, aby dany pracownik podjął działania i zgłosił takie sytuacje. Monitorowanie naruszające prawa pracowników do prywatności może utrudniać konieczną komunikację z odpowiednimi inspektorami. W takim przypadku ustanowione środki stosowane przez wewnętrznych demaskatorów mogą stracić na skuteczności.

## 2. Odpowiedzialność


### 2.1. Administrator Danych Osobowych [24]

jest odpowiedzialny za:



- 1) zapewnienie przetwarzania danych osobowych zgodnie z przepisami prawa, 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 i udowodnienie zgodności przetwarzania danych osobowych z przepisami prawa [24.1];

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
			Strona 19 z 81
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

- 2) identyfikacja celów przed rozpoczęciem przetwarzania i ich odpowiednich, zgodnych z prawem podstaw przetwarzania danych;
- 3) organizację bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami Rozporządzenia PE, Ustawy i wymaganiami innych przepisów prawnych dotyczących ochrony danych osobowych oraz sprawowanie nadzoru nad bezpieczeństwem danych osobowych przetwarzanych w Szpital Specjalistyczny w Prabutach Sp. z o.o. poprzez wprowadzenie odpowiednich środków technicznych i organizacyjnych adekwatnych do istotności ryzyka [32], aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania [25],
- 4) zarówno na etapie planowania sposobów przetwarzania, jak i w czasie samego przetwarzania, wdrażanie odpowiednich środków technicznych i organizacyjnych, mających na celu skuteczną realizację zasad ochrony danych oraz spełnienie wymogów Rozporządzenia PE, a także ochronę praw osób, których dane dotyczą; przy wdrożeniu takich rozwiązań ADO uwzględnia 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 wynikających z przetwarzania [25];
- 5) kierowanie się zasadą minimalizacji i zapewnienia prywatności na etapie projektowania mające zastosowanie do działalności całej organizacji, obejmujące swoim zakresem technologie informacyjne, procesy biznesowe i infrastrukturę sieciową, szczególnie na wstępnych etapach projektowania usług, produktów bądź systemów mających służyć do przetwarzania danych osobowych; koncepcja prywatności w fazie projektowania obejmuje: podejście proaktywne, niereaktywne i zaradcze, nie naprawcze; prywatność jako ustawienie domyślne; prywatność włączona w projekt; pełna funkcjonalność: suma dodatnia, a nie suma zerowa; ochrona od początku do końca cyklu życia informacji; widoczność i przejrzystość; poszanowanie dla prywatności użytkowników;
- 6) ciągły przegląd i uaktualnianie środków technicznych i organizacyjnych, o których mowa w art. 32 ust. 1 Rozporządzenia PE;
- 7) promowanie i przestrzeganie zasad systemu ochrony danych osobowych [5];
- 8) tworzenie polityk ochrony danych, ich aktualizacja i zapewnienie przetwarzania danych zgodnie z uregulowaniami POD [24],
- 9) wprowadzenie wewnętrznych zasad i procedur, które zapewnią wydajny i szybki przepływ informacji dotyczących ochrony danych [24];
- 10) akceptację dokumentów opisujących system ochrony danych osobowych [24];
- 11) prowadzenie rejestru czynności przetwarzania danych osobowych, za które odpowiada [30];
- 12) udział w procesie zarządzania ryzykiem poprzez akceptowanie ryzyk i działań redukujących ryzyka [32];
- 13) przeprowadzanie oceny skutków dla ochrony danych [35];

<p>Szpital Specjalistyczny w Prabutach sp. z o.o.</p>  <p>Podmiot Leczniczy Samorządu Województwa Pomorskiego</p>	<p><b>PROCEDURA</b></p>	<p>Wydanie: 3</p>	<p><b>10.08.2025</b></p>
		<p>Strona 20 z 81</p>	
<p><b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b></p>		<p>Nr dokumentu: <b>7- Pr5</b></p>	

- 14) konsultowanie się z organem nadzorczym zgodnie z art. 36 Rozporządzenia PE, przed rozpoczęciem przetwarzania, w przypadkach, gdy ocena skutków dla ochrony danych, o której mowa powyżej i w art. 35 Rozporządzenia PE, wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby ADO nie zastosował środków w celu zminimalizowania tego ryzyka;
- 15) jeżeli wymaga tego prawo [37], lub na zasadzie dobrowolności (w sytuacji, w której ADO dobrowolnie decyduje się na wyznaczenie IOD, wymagania wskazane w artykułach 37 - 39 Rozporządzenia PE stosuje się odpowiednio do jego wyznaczenia, statusu i zadań, tak jakby wyznaczenie było obowiązkowe) powołanie Inspektora Ochrony Danych, który bezpośrednio podlega najwyższemu kierownictwu ADO oraz:
- zapewnienie, by IOD był właściwie i niezwłocznie włączany w spotkania przedstawicieli wyższego i średniego szczebla organizacji w zakresie ochrony danych osobowych,
  - zapewnienie uczestnictwa IOD przy podejmowaniu decyzji dotyczących przetwarzania danych osobowych (niezbędne informacje powinny zostać udostępnione IOD odpowiednio wcześniej, umożliwiając IOD zajęcie stanowiska),
  - zapewnienie IOD uczestnictwa we wszystkich sprawach dotyczących ochrony danych osobowych,
  - branie pod uwagę stanowiska IOD i dokumentowanie przypadków i powodów postępowania niezgodnego z zaleceniem IOD,
  - niezwłoczne konsultowanie się z IOD w przypadku stwierdzenia naruszenia albo innego zdarzenia związanego z danymi osobowymi,
  - wspieranie IOD w wypełnianiu przez niego zadań, o których mowa w art. 39 Rozporządzenia PE,
  - zapewnienie IOD zasobów niezbędnych do wykonania w/w zadań,
  - zapewnienie IOD dostępu do danych osobowych i operacji przetwarzania,
  - zapewnienie IOD zasobów niezbędnych do utrzymania jego wiedzy fachowej,
  - zapewnienie by IOD nie otrzymywał instrukcji dotyczących wykonywania jego zadań,
  - zapewnienie, by IOD działał w sposób w pełni niezależny,
  - zapewnienie, by IOD nie został odwołany ani ukarany za wypełnianie jego zadań,
  - zapewnienie by inne zadania i obowiązki, które może wykonywać IOD nie powodowały konfliktu interesów, bowiem IOD nie może zajmować w organizacji stanowiska pociągającego za sobą określanie sposobów i celów przetwarzania danych,
  - zapewnienie poufności komunikacji z IOD,
  - publikowanie danych kontaktowych IOD,
  - zawiadomienie organu nadzorczego o danych kontaktowych IOD;
- 16) podejmowanie działań w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia ADO, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie ADO, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego [29];

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
			Strona 21 z 81
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	



- 17) powoływanie Zespołu ds. bezpieczeństwa danych osobowych w przypadku wystąpienia incydentu bezpieczeństwa oraz akceptację działań korygujących w przypadku wystąpienia incydentu bezpieczeństwa;
- 18) w przypadku naruszenia ochrony danych osobowych, zgłaszanie takiego naruszenia do Urzędu Ochrony Danych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych;
- 19) dokumentowanie, zgodnie z zasadą rozliczalności, w sposób przejrzysty i umożliwiający Urzędowi Ochrony Danych weryfikowanie przestrzegania art. 33 Rozporządzenia PE, wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutków oraz podjętych działań zaradczych;
- 20) jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, zawiadomienie bez zbędnej zwłoki osoby, której dane dotyczą, o takim naruszeniu, tak aby umożliwić jej podjęcie niezbędnych działań zapobiegawczych [34];
- 21) powiadamianie o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania [19]:
  - informowanie o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych osobowych – czego ADO dokonał zgodnie z art. 16, 17 ust. 1 i 18 Rozporządzenia PE – każdego odbiorcy, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku,
  - informowanie osoby, której dane dotyczą, o odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda;
- 22) zawieranie umów powierzenia danych osobowych z podmiotami przetwarzającymi [28],
- 23) współpraca z organem nadzorczym w ramach wykonywania przez niego swoich zadań oraz – gdy ma to zastosowanie – współpraca przedstawicieli ADO na żądanie organu nadzorczego [31];
- 24) udzielanie odpowiedzi na skargi w zakresie ochrony danych osobowych,
- 25) akceptowanie Sprawozdania z funkcjonowania systemu ochrony danych osobowych.

## **2.2. Inspektor ochrony danych [37-39]**

Administrator Danych wyznaczył Inspektora Ochrony Danych (IOD), który w jego imieniu realizował będzie funkcję i zadania osoby nadzorującej przestrzeganie zasad ochrony danych osobowych – zgodnie z art. 39 Rozporządzenia PE,

**Inspektor ochrony danych [39]** ma następujące zadania:

- 1) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego Rozporządzenia PE oraz przepisów prawa krajowego dotyczących ochrony danych osobowych;

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Lecznicy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
			Strona 22 z 81
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

- 2) monitorowanie przestrzegania Rozporządzenia PE oraz przepisów prawa krajowego dotyczących ochrony danych osobowych, a także polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty. W ramach monitorowania przestrzegania przepisów IOD może między innymi:
  - zbierać informacje w celu identyfikacji procesów przetwarzania,
  - analizować i sprawdzać zgodność tego przetwarzania,
  - informować, doradzać i rekomendować określone działania administratorowi albo podmiotowi przetwarzającemu;
- 3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 Rozporządzenia PE, jeżeli ma zastosowanie;
- 4) współpraca z organem nadzorczym;
- 5) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 Rozporządzenia PE oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.


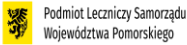
W zakresie pkt. 4 i 5 (powyżej) IOD pełni funkcję punktu kontaktowego, by umożliwić organowi nadzorczemu dostęp do dokumentów i informacji w celu realizacji zadań, o których mowa w art. 57 Rozporządzenia PE, jak również wykonywania uprawnień w zakresie prowadzonych postępowań, uprawnień naprawczych, uprawnień w zakresie wydawania zezwoleń oraz uprawnień doradczych, zgodnie z art. 58 Rozporządzenia PE.

IOD ma możliwość kontaktowania się w celu uzyskania porady ze strony organu nadzorczego. Art. 39 ust. 1 pkt. e Rozporządzenia PE stanowi, iż IOD może konsultować się z organem nadzorczym we wszystkich sprawach, w stosownych przypadkach.



IOD odgrywa rolę pośrednika pomiędzy zainteresowanymi stronami (np. organem ochrony danych osobowych, osobami, których dane dotyczą albo jednostkami w ramach przedsiębiorstwa).

Inspektor ochrony danych wypełnia swoje zadania z należyтым uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania. Wymaga to od IOD ustalania priorytetów w swojej pracy i koncentrowania się na aspektach pociągających za sobą większe ryzyko w zakresie ochrony danych. Nie oznacza to, iż dozwolone jest zaniedbywanie kontroli zgodności operacji przetwarzania danych o niższym ryzyku, a jedynie wskazuje słuszność skupienia się, przede wszystkim, na kwestiach o wyższym ryzyku.

- 6) realizowanie obowiązków informacyjnych [12-14],
- 7) prowadzenie korespondencji w imieniu ADO z osobą, której dane dotyczą [15-22 i 34]
- 8) współtworzenie polityk ochrony danych, ich aktualizacja i kontrola przetwarzania danych zgodnie z uregulowaniami POD,
- 9) egzekwowanie przestrzegania zasad ochrony danych,

 Szpital Specjalistyczny w Prabutach sp. z o.o.	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
		Strona 23 z 81	
 Podmiot Leczniczy Samorządu Województwa Pomorskiego	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

- 10) promowanie zasad dotyczących przetwarzania danych osobowych [5],
- 11) inicjowanie działań zmierzających do zapewnienia należytej ochrony danych osobowych,
- 12) prowadzenie w imieniu ADO Rejestru czynności przetwarzania (Form.3A/POD – Rejestr czynności przetwarzania) [30], który umożliwia ADO i organowi nadzorcemu (na wniosek) kontrolę wszystkich procesów przetwarzania danych w danej organizacji,
- 13) ocena skuteczności zastosowanych środków ochrony oraz rekomendowanie zmian,
- 14) koordynowanie procesu identyfikacji i analizy ryzyka utraty bezpieczeństwa danych osobowych przetwarzanych wykonywanych przez komórki organizacyjne, monitorowanie wdrożonych zabezpieczeń w celu ochrony danych osobowych, jeżeli uzna, że zarządzanie ryzykiem jest konieczne [32], w szczególności identyfikowanie ryzyka związanego z przetwarzaniem, jego oceny pod kątem źródła, charakteru, prawdopodobieństwa i wagi zagrożenia oraz wprowadzania skutecznych praktyk pozwalających zminimalizować to ryzyko,
- 15) przygotowanie analiz z procesu zarządzania ryzykiem [32],
- 16) dokumentowanie wszelkich naruszeń ochrony danych osobowych [33], w tym: prowadzenie postępowania wyjaśniającego, okoliczności wystąpienia incydentu lub/i naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze i przedstawianie ustaleń do akceptacji ADO,
- 17) prowadzenie w imieniu ADO korespondencji z organem nadzorczym w zakresie naruszeń [33],
- 18) przygotowanie powiadomienia do odbiorców o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania [19],
- 19) uwzględnianie ochrony danych w fazie projektowania rozwiązań technicznych bądź organizacyjnych (ze szczególnym uwzględnieniem zasady minimalizacji) oraz domyślna ochrona danych [25],
- 20) rekomendowanie ADO wdrażania odpowiednich środków technicznych i organizacyjnych podczas określania sposobów przetwarzania oraz w czasie samego przetwarzania [25] oraz nadzór i aktualizacja w/w środków; przy rekomendacji co do wdrożenia takich rozwiązań IOD uwzględnia 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 wynikające z przetwarzania,
- 21) organizowanie okresowych szkoleń z zakresu przetwarzania i ochrony danych osobowych oraz wymagań Rozporządzenia PE [39], w tym dla osób przed przyznaniem upoważnienia do przetwarzania danych osobowych,
- 22) prowadzenie ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych (Form.2/POD – Rejestr osób upoważnionych do przetwarzania danych osobowych),
- 23) nadzorowanie aktualności przyznanych upoważnień do przetwarzania danych osobowych w związku ze zmianami kadrowymi [29],
- 24) opiniowanie i tworzenie wzorów umów, odpowiadających wszystkim wymagom przewidzianym w art. 28–29 Rozporządzenia PE,



 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Lecznicy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
		Strona 24 z 81	
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

- 25) przygotowywanie umów powierzenia danych osobowych z podmiotami przetwarzającymi [28] oraz prowadzenie rejestru takich umów zgodnie z Form.8/POD,
- 26) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania (audyt wewnętrzny systemu danych osobowych) [39],
- 27) przygotowanie na Form.6/POD – Planu audytów wewnętrznych systemu ochrony danych osobowych,
- 28) przygotowanie na Form.5/POD – Roczno sprawozdania z funkcjonowania systemu ochrony danych osobowych i bezpieczeństwa informacji,
- 29) współpracę z Prezesem Urzędu Ochrony Danych Osobowych [39], w tym w zakresie składanych skarg [77],
- 30) zgłaszanie do ASI (informatyka Szpitala Specjalistycznego w Prabutach Sp. z o.o.) każdego nowego pracownika celem nadania mu uprawnień do systemów informatycznych oraz zgłaszanie każdej zakończonej umowy z pracownikiem lub osobami zatrudnionymi w Szpitalu Specjalistycznym w Prabutach Sp. z o.o. na innej podstawie niż umowa o pracę celem zablokowania kont tych osób w systemach informatycznych.

### **2.3. Użytkownik (kierownik komórki organizacyjnej, pracownik, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilnoprawnej)**

jest odpowiedzialny za:

- 1) realizację zadań wynikających z POD,
- 2) identyfikację zbiorów danych osobowych, ustalanie celów przetwarzania zbioru danych w swoim zakresie odpowiedzialności oraz niezwłoczne zgłaszanie nowych zbiorów do IOD,
- 3) zgłaszanie do IOD wszystkich zawieranych umów o świadczenie usług z podmiotami zewnętrznymi, gdzie przekazywane są dane osobowe na zewnątrz,
- 4) identyfikacja ryzyk w systemie ochrony danych osobowych oraz prowadzenie w komórce procesów zarządzania ryzykiem zgodnie z procedurą, która zawarta jest w POD wraz z załącznikiem (Form.4/POD – Arkusz ryzyka w ochronie danych osobowych),
- 5) zachowanie szczególnej staranności przy gromadzeniu danych osobowych i informacji, aby dane te były:
  - przetwarzane zgodnie z prawem oraz zasadami przetwarzania danych [5],
  - zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
  - merytorycznie poprawne i adekwatne w stosunku do celów, jakich są przetwarzane,
- 6) przestrzeganie zasad wskazanych w pkt. 1.4 i 11 POD,
- 7) zgłaszanie IOD/ADO wszelkich zauważonych nieprawidłowości dotyczących ochrony danych osobowych przetwarzanych w systemach informatycznych i w tradycyjnej papierowej formie oraz incydentów związanych z naruszeniem ochrony danych osobowych,



 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
			Strona 25 z 81
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

- 8) poprawne korzystanie z aplikacji zgodnie z powierzonymi obowiązkami służbowymi;
- 9) informowanie IOD/ADO, ASI (informatyk Szpital Specjalistyczny w Prabutach Sp. z o.o.) o wszelkich nieprawidłowościach działania systemów w których przetwarzane są dane osobowe,
- 10) ustalenie hasła, okresowe zmiany haseł,
- 11) utrzymywanie w ścisłej tajemnicy haseł, którymi się posługuje,
- 12) zmianę hasła w przypadku powzięcia przez użytkownika podejrzenia lub stwierdzenia, że z hasłem mogły zapoznać się osoby trzecie i powiadomienie o tym fakcie ADO.
- 13) **Kierownik komórki Kadr i Płac** – niezwłoczne zgłaszanie do IOD/ADO:
  - każdego nowego pracownika i osób zatrudnionych na umowę zlecenie lub inną cywilnoprawną, w Szpitalu Specjalistycznym w Prabutach Sp. z o.o.,
  - każdego przypadku zakończenia umowy z pracownikiem lub osobami zatrudnionymi w Szpitalu Specjalistycznym w Prabutach Sp. z o.o. na innej podstawie niż umowa o pracę.
  - zgłaszanie do ASI (informatyka Szpitala Specjalistycznego w Prabutach Sp. z o.o.) każdego nowego pracownika celem nadania mu uprawnień do systemów informatycznych oraz zgłaszanie każdej zakończonej umowy z pracownikiem lub osobami zatrudnionymi w Szpitalu Specjalistycznym w Prabutach Sp. z o.o. na innej podstawie niż umowa o pracę celem zablokowania kont tych osób w systemach informatycznych.

## **2.4. Odpowiedzialność Administratora Systemów Informatycznych**

– Informatyka Szpital Specjalistyczny w Prabutach Sp. z o.o. (skrót: ASI):

- 1) realizacja zadań wynikających z POD,
- 2) wykonywanie poleceń IOD/ADO w zakresie zadań związanych z ochroną danych osobowych i bezpieczeństwem informacji w systemach teleinformatycznych,
- 3) przyznawanie na wniosek IOD/ADO ściśle określonych praw dostępu do danych osobowych w poszczególnych systemach informatycznych,
- 4) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji w systemach teleinformatycznych,
- 5) zgłaszanie do IOD/ADO każdego incydentu bezpieczeństwa danych osobowych//informacji lub zdarzeń potencjalnie naruszających bezpieczeństwo przetwarzanych danych osobowych/informacji,
- 6) udział w identyfikacji i analizie ryzyka utraty bezpieczeństwa danych osobowych/informacji/aktywów przetwarzanych w Szpital Specjalistyczny w Prabutach Sp. z o.o. oraz monitorowanie wdrożonych zabezpieczeń dla IT w celu ochrony danych osobowych,
- 7) bezpośredni i osobisty nadzór nad instalacją oprogramowania,
- 8) zarządzanie i nadzorowanie sieci, w których przetwarzane są informacje,


 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Lecznicy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
		Strona 26 z 81	
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

- 9) rejestrowanie wszystkich zdarzeń w Dzienniku Administratora (Form 12/POD) takich jak m.in. konserwacja, naprawa sprzętu, przeglądy, wizyty zewnętrznych dostawców, administratorów, operatorów, incydenty bezpieczeństwa. Zapisów dokonuje się trwałym środkiem pisarskim. Dziennik Administratora pozostaje w dyspozycji Informatyka Szpitala Specjalistycznego w Prabutach Sp. z o.o.. Dziennik Administratora jest systematycznie przeglądany i analizowany.

## 2.5. Odpowiedzialność ADO jako Podmiotu Przetwarzającego [28]



W przypadku, gdy Szpital Specjalistyczny w Prabutach Sp. z o.o. przetwarza dane w imieniu innego administratora, wówczas jest Podmiotem Przetwarzającym (dalej PP) i jako taki ma następujące obowiązki:

- 1) Przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega PP; w takim przypadku przed rozpoczęciem przetwarzania PP informuje administratora 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) Przestrzega warunków korzystania z usług innego podmiotu przetwarzającego tj.:
  - a) nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody PP informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian;
  - b) korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi Rozporządzenia PE i chroniło prawa osób, których dane dotyczą;
  - c) jeżeli do wykonania w imieniu administratora konkretnych czynności przetwarzania PP korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają – na mocy umowy lub innego aktu prawnego (Umowa lub inny akt prawny, mają formę pisemną, w tym formę elektroniczną), które podlegają prawu Unii lub prawu państwa członkowskiego – te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między administratorem a podmiotem przetwarzającym, o których to obowiązkach mowa w ust. 3 Rozporządzenia PE, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom niniejszego rozporządzenia. Jeżeli ten inny podmiot przetwarzający nie

<p>Szpital Specjalistyczny w Prabutach sp. z o.o.</p>  <p>Podmiot Leczniczy Samorządu Województwa Pomorskiego</p>	<p>PROCEDURA</p>	<p>Wydanie: 3</p>	<p><b>10.08.2025</b></p>
		<p>Strona 27 z 81</p>	
	<p>POLITYKA OCHRONY DANYCH OSOBOWYCH</p>	<p>Nr dokumentu: <b>7- Pr5</b></p>	

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.

- 4) Biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III Rozporządzenia PE.
- 5) Uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36 Rozporządzenia PE.
- 6) Po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
- 7) Udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia PE oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.
- 8) PP niezwłocznie informuje administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie Rozporządzenia PE lub innych przepisów Unii lub państwa członkowskiego o ochronie danych.
- 9) Jeżeli PP naruszy Rozporządzenie PE przy określaniu celów i sposobów przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania.
- 10) Prowadzi rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, który ma formę pisemną, w tym formę elektroniczną zawierającą następujące informacje:
  - a) 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;
  - b) kategorie przetwarzania dokonywanych w imieniu każdego z administratorów;
  - c) gdy ma to zastosowanie – przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazania, o których mowa w art. 49 ust. 1 akapit drugi Rozporządzenia PE, dokumentacja odpowiednich zabezpieczeń;
  - d) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 Rozporządzenia PE.
- 11) Udostępnia rejestr na żądanie organu nadzorczego.
- 12) Współpracuje z organem nadzorczym w ramach wykonywania przez niego swoich zadań.

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
		Strona 28 z 81	
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	



- 13) Podejmuje wszelkie środki wymagane na mocy art. 32 Rozporządzenia PE - 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, PP wdraża odpowiednie 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.
- 14) Oceniając, czy stopień bezpieczeństwa jest odpowiedni, PP uwzględnia 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.
- 15) PP po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.
- 16) PP zobowiązuje się do niezwłocznego poinformowania administratora o jakimkolwiek postępowaniu administracyjnym lub sądowym, decyzji administracyjnej, orzeczeniu, zapowiedzianych kontrolach i inspekcjach, jeśli dotyczą one danych osobowych powierzonych przez administratora.

### **3. Prawa osób, których dane są przetwarzane**

Prawa osób, których dane są przetwarzane opisane są w Rozporządzeniu PE. ADO jest odpowiedzialny za przestrzeganie praw osób oraz odpowiednie reagowanie na uzasadnione żądania osób, których dane są przetwarzane.

Gdy osoba realizuje jakiegokolwiek swoje prawo, czyni to bez uszczerbku dla każdego innego prawa.


ADO podczas zbierania i przetwarzania danych osoby, której dane dotyczą, nie wykorzystuje otrzymanych od tej osoby, danych stron trzecich do własnych celów. Przetwarzanie takich danych osobowych jest dozwolone tylko w zakresie, w jakim dane są przechowywane pod wyłączną kontrolą osoby, której dane dotyczą i są przetwarzane tylko na potrzeby o czysto osobistym lub domowym charakterze. Informacje te nie będą również wykorzystane do uzyskania informacji na temat takich stron trzecich oraz tworzenia określonych profili, nawet jeżeli ich dane osobowe już są w posiadaniu ADO.

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
		Strona 29 z 81	
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

### 3.1. Obowiązki informacyjne


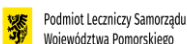
#### 3.1.1. Przejrzyste informowanie i przejrzysta komunikacja oraz tryb wykonywania praw przez osobę, której dane dotyczą [12]

- 1) Jeżeli osoba, której dane są przetwarzane zwróci się do Szpitala Specjalistycznego w Prabutach Sp. z o.o. z żądaniem potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz otrzymania informacji o przetwarzanych danych.
- 2) ADO udziela wszelkich informacji, o których mowa w art. 13 i 14 Rozporządzenia PE, oraz prowadzi z osobą, której dane dotyczą, wszelką komunikację na mocy art. 15–22 i 34 Rozporządzenia PE w sprawie przetwarzania.
- 3) ADO udziela odpowiedzi w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności gdy informacje są kierowane do dziecka, bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania.
- 4) W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. 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.
- 5) Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.
- 6) ADO ułatwia osobie, której dane dotyczą, wykonanie praw przysługujących jej na mocy art. 15–22 Rozporządzenia PE i nie odmawia podjęcia działań na żądanie osoby której dane dotyczą pragnącej wykonać te prawa, chyba że wykaże, iż nie jest w stanie zidentyfikować osoby, której dane dotyczą [11.2]. Zgodnie z art. 11 ust. 1 Rozporządzenia PE jeżeli cele, w których ADO przetwarza dane osobowe, nie wymagają lub już nie wymagają zidentyfikowania przez niego osoby, której dane dotyczą, ADO nie ma obowiązku zachowania, uzyskania ani przetworzenia dodatkowych informacji w celu zidentyfikowania osoby, której dane dotyczą, wyłącznie po to, by zastosować się do Rozporządzenia PE.
- 7) Jednak jeżeli ADO może wykazać, że nie jest w stanie zidentyfikować osoby, której dane dotyczą, w miarę możliwości informuje o tym osobę, której dane dotyczą. W takich przypadkach zastosowania nie mają art. 15–20 Rozporządzenia PE, chyba że osoba, której dane dotyczą, w celu wykonania praw przysługujących jej na mocy tych artykułów dostarczy dodatkowych informacji pozwalających ją zidentyfikować [11.2].
- 8) Jeżeli ADO ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, o którym mowa w art. 15–21 Rozporządzenia PE, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą. Jeżeli

<p>Szpital Specjalistyczny w Prabutach sp. z o.o.</p>  <p>Podmiot Leczniczy Samorządu Województwa Pomorskiego</p>	PROCEDURA	Wydanie: 3	<b>10.08.2025</b>
			Strona 30 z 81
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

osoba, której dane dotyczą, przekaze dodatkowe informacje umożliwiające jej identyfikację, ADO nie może odmówić realizacji wniosku.

- 9) Osoba, której dane dotyczą może złożyć wniosek do ADO korzystając z przysługujących jej praw. W zakres takiego wniosku wchodzić mogą tylko dane osobowe dotyczące osoby, której dane dotyczą. W związku z tym wszelkie dane będącymi danymi anonimowymi lub nie dotyczącymi osoby, której dane dotyczą, nie będą wchodziły w ten zakres. Jednak dane poddane pseudonimizacji, które można wyraźnie powiązać z osobą, której dane dotyczą (np. poprzez podanie przez nią odnośnego identyfikatora, por. artykuł 11 ust. 2 Rozporządzenia PE), mieszczą się w tym zakresie. Jeżeli ADO przetwarza informacje, które zawierają dane osobowe kilku osób, których dane dotyczą, wówczas nie przyjmuje zbyt wąskiej interpretacji zdania „dane osobowe dotyczące osoby, której dane dotyczą”.
- 10) Prawa osoby, której dane dotyczą obejmują dane przekazane świadomie i aktywnie przez osobę, której dane dotyczą, jak również dane osobowe wygenerowane poprzez jej działanie, w związku z korzystaniem z usługi lub urządzenia. Dane wywnioskowane i dane wywiedzione tworzone są przez ADO na podstawie danych „przekazanych przez osobę, której dane dotyczą” nie będą jako takie uznane za „przekazane przez” osobę, której dane dotyczą. Termin „przekazane przez osobę, której dane dotyczą” ADO interpretuje szeroko, z wyłączeniem tylko „danych wywnioskowanych” i „danych wywiedzionych”, które obejmują dane osobowe, które są tworzone przez dostawcę usług. ADO może wyłączyć takie wywnioskowane dane, ale powinien uwzględnić wszystkie inne dane osobowe przekazane przez osobę, której dane dotyczą, za pomocą środków technicznych zapewnionych przez ADO. Zatem termin „przekazane przez” obejmuje dane osobowe, które dotyczą działania osoby, której dane dotyczą, lub wyniku z obserwacji zachowania osoby, ale nie obejmuje danych wynikających z następującej analizy tego zachowania. Z drugiej strony, wszelkie dane osobowe, które zostały wytworzone przez ADO w ramach przetwarzania danych, np. przez proces personalizacji lub rekomendacji, przez kategoryzację użytkownika lub profilowanie, to dane, które są wywiedzione lub wywnioskowane z danych osobowych przekazanych przez osobę, której dane dotyczą, i nieobjęte prawami osoby, której dane dotyczą.
- 11) Gdy informacje i dane zebrane online są powiązane z pseudonimami lub unikalnymi identyfikatorami, ADO może wdrożyć odpowiednie procedury uwierzytelniania w celu zdecydowanego potwierdzenia tożsamości osoby, której dane dotyczą, wnioskującej o swoje dane osobowe lub bardziej ogólnie realizującej prawa przyznane przez Rozporządzenie PE. Jeżeli osoby, których dane dotyczą, zostały uwierzytelnione w systemie ADO przed przetwarzaniem, wówczas w konsekwencji dane osobowe wykorzystywane do rejestracji osoby, której dotyczy przetwarzanie, mogą być również wykorzystane jako dowód uwierzytelnienia osoby, której dane dotyczą. Podczas, gdy w tych przypadkach uprzednia identyfikacja osób, których dane dotyczą, może wymagać żądania przedstawienia dowodu potwierdzającego ich tożsamość prawną, taka weryfikacja może nie być właściwa do oceny powiązania między danymi a osobą, której sprawa dotyczy, ponieważ takie



 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	PROCEDURA	Wydanie: 3	10.08.2025
			Strona 31 z 81
	POLITYKA OCHRONY DANYCH OSOBOWYCH	Nr dokumentu: <b>7- Pr5</b>	

powiązanie nie jest związane z tożsamością oficjalną czy też prawną. W istocie możliwość żądania przez ADO dodatkowych informacji w celu oceny tożsamości nie może prowadzić do nadmiernych żądań i do zbierania danych osobowych, które nie są istotne czy niezbędne do wzmocnienia powiązania między osobą a żądanymi danymi osobowymi.

- 12) Jeżeli rozmiar danych wnioskowanych, na podstawie art. 15 lub 20 Rozporządzenia PE, przez osobę, której dane dotyczą, powoduje, że ich przesłanie za pośrednictwem Internetu może być problematyczne, zamiast możliwości przedłużenia terminu udzielenia odpowiedzi na wniosek o maksymalnie trzy miesiące, ADO może również rozważyć alternatywne środki przekazania danych, takie jak „streaming” lub zapisanie na płycie CD, DVD lub innym fizycznym nośniku bądź też pozwolić na przesłanie danych osobowych bezpośrednio innemu administratorowi danych (zgodnie z art. 20 ust. 2 Rozporządzenia PE, gdy jest to technicznie wykonalne).
- 13) Informacje podawane na mocy art. 13 i 14 Rozporządzenia PE oraz komunikacja i działania podejmowane na mocy art. 15–22 i 34 Rozporządzenia PE są wolne od opłat.
- 14) Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, ADO może pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań albo odmówić podjęcia działań w związku z żądaniem.
- 15) Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na ADO. W tym celu ADO gromadzi niezbędną dokumentację i przygotowuje wyjaśnienie/opinię zgodnie z zasadą rozliczalności.
- 16) W rzeczywistości powinno być niewiele przypadków, w których administrator danych byłby w stanie uzasadnić odmowę dostarczenia wnioskowanych informacji, nawet w odniesieniu do wielu wniosków o przeniesienie danych. Ponadto całkowity koszt procedur ustanowionych w celu udzielania odpowiedzi na wnioski o przeniesienie danych nie powinien być brany pod uwagę przy określaniu „nadmiernego charakteru” wniosku. W rzeczywistości art. 12 Rozporządzenia PE koncentruje się na wnioskach składanych przez jedną osobę, której dane dotyczą, a nie na łącznej liczbie wniosków otrzymanych przez administratora danych. W rezultacie całkowitymi kosztami wdrożenia systemu nie można obciążać osób, których dane dotyczą, ani nie mogą one być używane do uzasadnienia odmowy udzielenia odpowiedzi na wnioski o przeniesienie.
- 17) Jeżeli ADO nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

### 3.1.2. Obowiązek informacyjny odnośnie prawa do sprzeciwu [21]

- 1) W przypadku, gdy ADO zamierza przetwarzać lub przetwarza dane osobowe na podstawie:

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
			Strona 32 z 81
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

- a) art. 6 ust. 1 lit. e) Rozporządzenia PE, gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej ADO lub,
- b) art. 6 ust. 1 lit. f) Rozporządzenia PE, gdy 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, wówczas najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, ADO wyraźnie informuje ją o prawie do sprzeciwu obowiązkowo informacyjnym w zapisie:


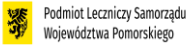
Posiada Pani/Pan prawo dostępu do swoich danych, ich sprostowania, usunięcia, ograniczenia przetwarzania a także prawo do wniesienia sprzeciwu wobec przetwarzania oraz do przenoszenia danych, przy czym zgodnie z art. 17 ust. 3 RODO prawo do wniesienia sprzeciwu nie ma zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:

- a) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa polskiego;
- b) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO, o ile prawdopodobne jest, że prawo sprzeciwu, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania;
- c) do ustalenia, dochodzenia lub obrony roszczeń.

### **3.1.3. Klauzula Informacyjna [13-14]**

ADO przed pozyskaniem danych ocenia cele, dla których dane mają być faktycznie przetwarzane oraz legalne podstawy tego przetwarzania.

ADO, aby przetwarzać dane osobowe zgodnie z prawem, gromadzi, w sposób przejrzysty dla osoby, której dane dotyczą, tylko te prawidłowe i w razie potrzeby uaktualniane dane osobowe, które są zasadniczo rzetelne, niezbędne i konieczne w odniesieniu do konkretnych, wyraźnych i prawnie uzasadnionych celów przetwarzania. ADO nie przetwarza dalej w sposób niezgodny z tymi celami. ADO wykazuje, że 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. ADO

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	PROCEDURA	Wydanie: 3	<b>10.08.2025</b>
			Strona 33 z 81
	POLITYKA OCHRONY DANYCH OSOBOWYCH	Nr dokumentu: <b>7- Pr5</b>	

przechowuje dane osobowe w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.

W celu zapewnienia zgodności z artykułami 13 i 14 Rozporządzenia PE, ADO przedstawia osobie, której dane dotyczą, informacje wymagane w/w artykułami oraz pełną listę odbiorców lub kategorii odbiorców, w tym podmiotów przetwarzających.

W zależności od okoliczności i kontekstu sprawy, ADO przedstawia więcej potrzebnych informacji, aby pozwolić osobie, której dane dotyczą, rzeczywiście zrozumieć operacje przetwarzania.



Jeżeli ADO planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji zgodnie z art. 13 lub 14 Rozporządzenia PE.

ADO, o każdej zmianie podstawy przetwarzania, informuje osobę, której dane dotyczą, zgodnie z wymogami dotyczącymi informacji zawartymi w art. 13 lub 14 Rozporządzenia PE i zgodnie z ogólną zasadą przejrzystości.

**1. Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby [13], ADO podczas pozyskiwania danych osobowych (przy pierwszym kontakcie) przedkłada jej do podpisu dokument, który zawiera następujące informacje:**

- a) swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;*
- b) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych;*
- c) cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;*
- d) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) RODO – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;*
- e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;*
- f) 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 RODO akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.*



**2. Poza informacjami, o których mowa w pkt. 1, podczas pozyskiwania danych osobowych administrator podaje osobie, której dane dotyczą, następujące inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania:**

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Lecznicy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
		Strona 34 z 81	
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

- a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
  - b) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
  - c) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) 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;
  - d) informacje o prawie wniesienia skargi do organu nadzorczego;
  - e) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
  - f) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO 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.
3. Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w pkt. 2. 4. Pkt. 1, 2 i 3 nie mają zastosowania, gdy – i w zakresie, w jakim – osoba, której dane dotyczą, dysponuje już tymi informacjami.

**2. W przypadku zbierania danych osobowych w inny sposób, niż od osoby, której dane dotyczą [14] ADO przedkłada osobie, której dane dotyczą, do podpisu który zawiera następujące informacje:**

- a) swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
- b) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych;
- c) cele przetwarzania, do których mają posłużyć dane osobowe, oraz podstawę prawną przetwarzania;
- d) kategorie odnośnych danych osobowych;
- e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
- f) 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 RODO akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
		Strona 35 z 81	
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

2. Poza informacjami, o których mowa w pkt. 1, administrator podaje osobie, której dane dotyczą, następujące informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania wobec osoby, której dane dotyczą:

- a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
- b) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) RODO – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;
- c) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
- d) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) 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;
- e) informacje o prawie wniesienia skargi do organu nadzorczego;
- f) źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych;
- g) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, 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.



3. Informacje, o których mowa w pkt. 1 i 2, administrator podaje:

- a) w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych;
- b) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub
- c) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.

4. Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym te dane zostały pozyskane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w pkt. 2.

5. Pkt. 1– 4 nie mają zastosowania, gdy – i w zakresie, w jakim:

- a) osoba, której dane dotyczą, dysponuje już tymi informacjami;
- b) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku; w szczególności w przypadku przetwarzania do celów archiwalnych w

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Strona 36 z 81	
		Nr dokumentu: <b>7- Pr5</b>	


*interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1 RODO, lub o ile obowiązek, o którym mowa w pkt. 1 może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. W takich przypadkach administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnić informacje publicznie;*

*c) pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą; lub*


*d) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.*

## **Zgoda na przetwarzanie danych osobowych [7]**

- 1) Zgoda osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych, gdzie:
  - a) element „dobrowolna” oznacza rzeczywisty wybór i kontrolę zapewnione dla osoby, której dane dotyczą. Jeżeli osoba, której dane dotyczą, nie ma rzeczywistego wyboru, czuje się zmuszona do wyrażenia zgody lub poniesie negatywne konsekwencje, jeżeli nie wyrazi zgody, zgoda będzie nieważna. Jeżeli zgoda jest włączona jako niepodlegająca negocjacji część warunków, zakłada się, że nie została wyrażona dobrowolnie. W związku z tym zgoda nie będzie uznana za dobrowolną, jeżeli osoba, której dane dotyczą, nie ma możliwości odmówienia lub wycofania swojej zgody bez niekorzystnych konsekwencji. Aby zapewnić dobrowolność, zgoda nie powinna stanowić ważnej podstawy prawnej przetwarzania danych osobowych w szczególnej sytuacji, w której istnieje wyraźny brak równowagi między osobą, której dane dotyczą, a administratorem, w szczególności gdy administrator jest organem publicznym i dlatego jest mało prawdopodobne, by w tej konkretnej sytuacji zgodę wyrażono dobrowolnie we wszystkich przypadkach. W pracy zgoda pracowników (artykuł 6 ust. 1 lit. a Rozporządzenia PE) nie może i nie powinna być legalną podstawą ze względu na charakter relacji między pracodawcą a pracownikiem. Zważywszy na brak równowagi sił między pracodawcą a jego pracownikami, pracownicy mogą wyrazić dobrowolną zgodę tylko w wyjątkowych okolicznościach, gdy nie będzie to miało żadnych negatywnych konsekwencji, niezależnie od tego, czy wyrażą zgodę, czy też nie. Zgoda nie będzie dobrowolna w przypadkach, w których istnieje jakikolwiek element przymusu, nacisku lub braku możliwości wyrażenia wolnej woli. Administrator musi wykazać, że zgoda osoby, której dane dotyczą, była dobrowolna.


<p>Szpital Specjalistyczny w Prabutach sp. z o.o.</p>  <p>Podmiot Leczniczy Samorządu Województwa Pomorskiego</p>	<p><b>PROCEDURA</b></p>	<p>Wydanie: 3</p>	<p><b>10.08.2025</b></p>
		<p>Strona 37 z 81</p>	
<p><b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b></p>		<p>Nr dokumentu: <b>7- Pr5</b></p>	

- b) warunkowość – art. 7 ust. 4 Rozporządzenia PE wskazuje między innymi, że sytuacja „połączenia” zgody z akceptacją warunków lub „powiązanie” realizacji umowy lub usługi z zapytaniem o zgodę na przetwarzanie danych osobowych, które nie są niezbędne do realizacji tej umowy lub usługi, jest uznawane za wysoce niepożądane. Jeżeli zgoda jest wyrażana w takich okolicznościach, uważa się, że nie jest dobrowolna. Przetwarzanie danych osobowych, na które prosi się o zgodę, nie może stać się bezpośrednio lub pośrednio wspólną realizacją umowy. Dwie podstawy prawne legalnego przetwarzania danych osobowych, tj. zgoda i umowa, nie mogą być połączone ani niejasne. Jeżeli administrator chce przetwarzać dane osobowe, które są rzeczywiście niezbędne do wykonania umowy, istnieje prawdopodobieństwo, że prawidłową podstawą prawną jest artykuł 6 ust. 1 lit. b Rozporządzenia PE. Mogą niekiedy zdarzać się przypadki, w których warunkowość nie będzie powodować nieważności zgody, jednak ciężar dowodu będzie spoczywał na administratorze.
- c) szczegółowość - zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele. Usługa może obejmować liczne operacje przetwarzania dla więcej niż jednego celu. W takich przypadkach osoby, których dane dotyczą, powinny mieć raczej wolny wybór, jaki cel chcą zaakceptować, a nie mieć do czynienia z sytuacją, w której muszą zgodzić się na szereg celów przetwarzania. W danym przypadku można zagwarantować szereg zgód w celu rozpoczęcia oferowania usług. Zgody nie uważa się za dobrowolną, jeżeli proces/procedura uzyskania zgody nie pozwala osobom, których dane dotyczą, na wyrażenie odrębnej zgody na poszczególne operacje przetwarzania danych osobowych mimo, że w danym przypadku byłoby to stosowne.
- d) niekorzystne konsekwencje – administrator musi wykazać, że możliwe jest odmówienie lub wycofanie zgody bez niekorzystnych konsekwencji. Administrator powinien być w stanie udowodnić, że osoba, której dotyczą dane, mogła dokonać rzeczywistego, wolnego wyboru, czy wyrazić zgodę, i że możliwe było wycofanie zgody bez niekorzystnych konsekwencji.
- e) konkretna - wymóg, że zgoda musi być „konkretna” ma na celu zapewnienie stopnia kontroli użytkownika oraz przejrzystości dla osoby, której dane dotyczą. Aby zapewnić zgodność z elementem „konkretna”, ADO musi zastosować: (1) określenie celu jako zabezpieczenie przed rozrostem funkcji, (2) szczegółowość w zapytaniach o zgodę, oraz (3) wyraźne oddzielenie informacji związanych z uzyskaniem zgody na działania w zakresie przetwarzania danych od informacji dotyczących innych kwestii. Cel, który jest niejasny lub ogólny, jak na przykład „poprawienie doświadczenia użytkowników”, „cele marketingowe”, „cele bezpieczeństwa IT” lub „przyszłe badania”, zazwyczaj nie będzie – bez dalszych szczegółów – spełniał kryterium bycia „konkretnym”. Zgoda może obejmować różne operacje, o ile operacje te służą temu samemu celowi. Konkretna zgoda może być uzyskana tylko, jeżeli osoby, których dane dotyczą, zostaną konkretnie

<p>Szpital Specjalistyczny w Prabutach sp. z o.o.</p>  <p>Podmiot Leczniczy Samorządu Województwa Pomorskiego</p>	<p>PROCEDURA</p>	Wydanie: 3	10.08.2025
		Strona 38 z 81	
<p>POLITYKA OCHRONY DANYCH OSOBOWYCH</p>		Nr dokumentu: <b>7- Pr5</b>	

poinformowane o planowanych celach wykorzystywania dotyczących ich danych. Administrator, gdy prosi o zgodę do różnych celów, powinien zapewnić odrębną możliwość wyrażenia zgody (mechanizm opt-in) dla każdego celu, aby umożliwić użytkownikom wyrażenie konkretnej zgody na konkretne cele. Administrator powinien zapewnić wraz z każdym odrębnym zapytaniem o zgodę konkretne informacje na temat danych, które są przetwarzane w każdym celu, aby uświadomić osoby, których dane dotyczą, na temat skutków różnych wyborów, jakich mogą dokonać.

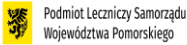
- f) świadoma - zapewnianie informacji osobom, których dane dotyczą, przed uzyskaniem ich zgody jest niezbędne do umożliwienia im podejmowania świadomych decyzji, zrozumienia, na co wyrażają zgodę, oraz na przykład realizacji ich prawa do wycofania zgody. Konsekwencją nieprzestrzegania wymogów świadomej zgody jest fakt, że zgoda będzie nieważna. Do uzyskania ważnej zgody wymagane są co najmniej następujące informacje: (1) tożsamość administratora, (2) cel każdej operacji przetwarzania, dla której prosi się o zgodę, (3) jakie dane (jaki rodzaj danych) będą zbierane i wykorzystywane, (4) istnienie prawa do wycofania zgody, (5) informacje na temat wykorzystywania danych do decyzji opartych jedynie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, zgodnie z art. 22 ust. 2 Rozporządzenia PE oraz (6) jeżeli zgoda dotyczy przekazywania – informacje na temat możliwych zagrożeń związanych z przekazywaniem danych do krajów trzecich w przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony oraz odpowiednich zabezpieczeń (art. 49 ust. 1 lit. a Rozporządzenia PE).
- g) jednoznaczne okazanie woli - zgoda wymaga oświadczenia od osoby, której dane dotyczą, lub wyraźnego działania potwierdzającego, co oznacza, że musi być zawsze udzielona poprzez aktywne działanie lub deklarację. Musi być oczywiste, że osoba, której dane dotyczą, zgodziła się na określone przetwarzanie. „Wyraźne działanie potwierdzające” oznacza, że osoba, której dane dotyczą, musiała podjąć celowe działanie w celu wyrażenia zgody na określone przetwarzanie. Zgodę można uzyskać w formie pisemnego lub (zarejestrowanego) ustnego oświadczenia, w tym drogą elektroniczną, choć należy wziąć pod uwagę informacje dostępne dla osoby, której dane dotyczą, przed wskazaniem zgody. Zastosowanie wcześniej zaznaczonych pól ze zgodą nie jest ważne na mocy Rozporządzenia PE. Milczenie lub bezczynność po stronie osoby, której dane dotyczą, jak również po prostu kontynuowanie usługi nie mogą być uznane za aktywne wskazanie wyboru. Administrator musi również być świadomy faktu, że zgoda nie może być uzyskana poprzez takie samo działanie jak zgoda na umowę lub akceptacja ogólnych warunków usługi. Ukryta akceptacja ogólnych warunków nie może być uznana za jasne działanie potwierdzające w celu wyrażenia zgody na wykorzystanie danych osobowych. Rozporządzenie PE nie pozwala na oferowanie wcześniej zaznaczonych pól lub mechanizmów opt-out (możliwość rezygnacji), które wymagają ingerencji ze strony osoby, której dane dotyczą, w celu uniemożliwienia zgody.

<p>Szpital Specjalistyczny w Prabutach sp. z o.o.</p>  <p>Podmiot Leczniczy Samorządu Województwa Pomorskiego</p>	<p><b>PROCEDURA</b></p>	<p>Wydanie: 3</p>	<p><b>10.08.2025</b></p>
		<p>Strona 39 z 81</p>	
<p><b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b></p>		<p>Nr dokumentu: <b>7- Pr5</b></p>	

h) uzyskanie wyraźnej zgody – termin „wyraźna” odnosi się do sposobu, w jaki zgoda jest wyrażana przez osobę, której dane dotyczą. Oznacza to, że osoba, której dane dotyczą, musi wyrazić oświadczenie zgody. Oczywistym sposobem zapewnienia tego wymogu jest uzyskanie potwierdzenia zgody w pisemnym oświadczeniu. Administrator mógłby zapewnić, gdy jest to właściwe, aby pisemne oświadczenie było podpisane przez osobę, której dane dotyczą, w celu usunięcia wszelkich możliwych wątpliwości i możliwego braku dowodów w przyszłości. Nie jest to jednak jedyny sposób uzyskania wyraźnej zgody na przykład w kontekście cyfrowym lub online osoba, której dane dotyczą, może być w stanie wydać wymagane oświadczenie, wypełniając formularz elektroniczny, wysyłając wiadomość e-mail, przesyłając zeskanowany dokument opatrzony podpisem osoby, której dane dotyczą, lub używając podpisu elektronicznego. W teorii wykorzystanie oświadczeń ustnych również być wystarczające do uzyskania ważnej wyraźnej zgody, jednak administratorowi trudno może być udowodnić, że spełniono wszystkie warunki ważnej wyraźnej zgody, gdy przyjmowano oświadczenie. Dwuetapowa weryfikacja zgody również może być sposobem na zapewnienie, że zgoda będzie ważna.

Wyraźna zgoda jest wymagana w określonych sytuacjach (patrz przepisy art. 9 Rozporządzenia PE dotyczących przetwarzania szczególnych kategorii danych, przepisach dotyczących przekazywania danych do państw trzecich lub organizacji międzynarodowych w przypadku braku odpowiednich zabezpieczeń w art. 49 Rozporządzenia PE oraz w art. 22 Rozporządzenia PE dotyczącym zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach, w tym profilowania), gdy pojawia się poważne zagrożenie ochrony danych, zatem gdy wysoki poziom kontroli osoby fizycznej nad danymi osobowymi jest uważany za odpowiedni.

- 2) Generalnie zgoda może być odpowiednią podstawą prawną tylko wówczas, jeżeli osoba, której dane dotyczą, ma zapewnioną możliwość sprawowania kontroli oraz rzeczywistą możliwość wyboru, jeżeli chodzi o zaakceptowanie lub odrzucenie proponowanych warunków lub też odrzucenie ich bez niekorzystnych konsekwencji. W przypadku proszenia o zgodę, ADO obowiązkowo ocenia, czy spełni wszystkie wymogi uzyskania ważnej zgody, by przetwarzać dane osobowe zgodnie z prawem na podstawie art. 6 ust. 1 lit. a Rozporządzenia PE. Jest to szczególnie ważne, ponieważ zazwyczaj zapytania o zgodę dotyczą działań, które co do zasady są nielegalne bez uzyskania zgody.
- 3) Biorąc pod uwagę powyższe, rozpoczynając działania obejmujące przetwarzanie danych osobowych, ADO zawsze rozważa, czy zgoda jest odpowiednią legalną podstawą przewidzianego przetwarzania lub czy zamiast tego należy wybrać inną podstawę.
- 4) ADO przed pozyskaniem danych ocenia cele, dla których dane są faktycznie przetwarzane oraz legalne podstawy tego przetwarzania.
- 5) ADO ważne informacje może przedstawić na różne sposoby, na przykład jako oświadczenia pisemne lub ustne, bądź też jako wiadomości w formacie audio lub wideo. Jednak prosząc o zgodę, ADO upewnia się, że używa jasnego i prostego języka we wszystkich przypadkach.


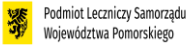
<p>Szpital Specjalistyczny w Prabutach sp. z o.o.</p>  <p>Podmiot Leczniczy Samorządu Województwa Pomorskiego</p>	PROCEDURA	Wydanie: 3	10.08.2025
		Strona 40 z 81	
	POLITYKA OCHRONY DANYCH OSOBOWYCH	Nr dokumentu: <b>7- Pr5</b>	

Oznacza to, że wiadomość powinna być zrozumiała dla przeciętnej osoby, a nie tylko dla prawników. ADO nie stosuje nieczytelnej polityki prywatności lub oświadczeń pełnych żargonu prawnego. Informacje istotne dla podejmowania świadomych decyzji, czy wyrazić zgodę czy nie, nie są ukryte w ogólnych warunkach. ADO zapewnia, że zgoda jest zapewniona na podstawie informacji, które pozwalają osobom, których dane dotyczą, łatwo określić, kto jest administratorem, i zrozumieć, na co wyrażają zgodę. ADO jasno opisuje cel przetwarzania danych, na które prosi o zgodę.

- 6) W zależności od okoliczności i kontekstu sprawy, ADO przedstawia więcej potrzebnych informacji, aby pozwolić osobie, której dane dotyczą, rzeczywiście zrozumieć operacje przetwarzania.

UWAGA: Osoby, których dane dotyczą, mają zostać konkretnie poinformowane o planowanych celach wykorzystywania dotyczących ich danych. ADO, gdy prosi o zgodę do różnych celów, zapewnia odrębną możliwość wyrażenia zgody dla każdego celu, aby umożliwić osobom, których dane dotyczą wyrażenie konkretnej zgody na konkretne cele. ADO zapewnia wraz z każdym odrębnym zapytaniem o zgodę konkretne informacje na temat danych, które są przetwarzane w każdym celu, aby uświadomić osoby, których dane dotyczą, na temat skutków różnych wyborów, jakich mogą dokonać. Jeżeli w danym przypadku jest to stosowne, ADO zapewnia osobom, których dane dotyczą, wyrażenie odrębnej zgody na poszczególne operacje przetwarzania danych osobowych)

- 7) ADO, aby przetwarzać dane osobowe zgodnie z prawem, gromadzi, w sposób przejrzysty dla osoby, której dane dotyczą, tylko te prawidłowe i w razie potrzeby uaktualniane dane osobowe, które są zasadniczo rzetelne, niezbędne i konieczne w odniesieniu do konkretnych, wyraźnych i prawnie uzasadnionych celów przetwarzania. ADO nie przetwarza dalej w sposób niezgodny z tymi celami. ADO wykazuje, że 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. ADO przechowuje dane osobowe w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.
- 8) Treść Zgody na przetwarzanie danych osobowych wyrażona powinna być w pisemnym oświadczeniu. Zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Lecznicy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
			Strona 41 z 81
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

- 9) ADO ma obowiązek wykazania, że osoba, której dane dotyczą, wyraziła zgodę. Obowiązek wykazania prawidłowo wyrażonej zgody istnieje dopóki dane są przetwarzane.
- 10) Jeżeli ADO przetwarza dane na podstawie zgody i chciałby przetwarzać dane w nowym celu, wówczas musi zwrócić się do osoby, której dane dotyczą, o nową zgodę na nowy cel przetwarzania, bowiem pierwotna zgoda nigdy będzie legitymizować nowych celów przetwarzania.
- 11) ADO aktualizuje zgodę w odpowiednich odstępach czasu. Jak długo ważna jest zgoda, będzie zależało od kontekstu, zakresu pierwotnej zgody i oczekiwań osób, których dane dotyczą. Jeśli operacje przetwarzania zmienią się lub ewoluują w sposób znaczący, wówczas pierwotna zgoda nie będzie dalej ważna. W takim przypadku ADO uzyskuje nową zgodę.
- 12) ADO bazując na zgodzie osoby, której dane dotyczą, jednocześnie przestrzega odrębnych obowiązków informacyjnych określonych w artykułach 13 i 14 Rozporządzenia PE.
- 13) W przypadku, gdy zgoda zostanie wycofana, ADO musi zaprzestać przetwarzania tych danych, powinny one zostać usunięte lub zanonimizowane. Chyba, że ADO wykaże istnienie innej zgodnej z prawem podstawy uzasadniającej przetwarzanie danych (np. dalsze przechowywanie). Istnienie takiej, innej zgodnej z prawem, podstawy uzasadniającej przetwarzanie danych ADO ustala i odpowiednio dokumentuje, zgodnie z zasadą rozliczalności.
- 14) W sytuacji gdy osoba, której dane dotyczą, wycofuje zgodę, a ADO planuje kontynuować przetwarzanie danych osobowych na innej podstawie, nie może on w milczeniu przejść ze zgody (która jest wycofana) na tę inną podstawę prawną. ADO, o każdej zmianie podstawy przetwarzania, informuje osobę, której dane dotyczą, zgodnie z wymogami dotyczącymi informacji zawartymi w art. 13 oraz 14 Rozporządzenia PE i zgodnie z ogólną zasadą przejrzystości.
- 15) Wszystkie operacje przetwarzania danych oparte na zgodzie, które miały miejsce przed jej wycofaniem – jeśli były zgodne z Rozporządzeniem PE – pozostają legalne.


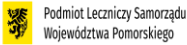
*Wyrażam zgodę/nie wyrażam zgody\* na przetwarzanie danych osobowych np. imię, nazwisko, pesel, adres, w tym szczególnych kategorii danych takich jak dane dotyczące stanu zdrowia dla celu .....*

*Oświadczam, że wyrażam zgodę na przetwarzanie moich danych osobowych dobrowolnie i zostałem poinformowany o możliwości wycofania mojej zgody w każdym czasie.*

.....



*(data i podpis)*

*\*niewłaściwe skreślić*

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	PROCEDURA	Wydanie: 3	10.08.2025
		Strona 42 z 81	
	POLITYKA OCHRONY DANYCH OSOBOWYCH	Nr dokumentu: <b>7- Pr5</b>	

### 3.2. Prawo dostępu przysługujące osobie, której dane dotyczą [15]

- 1) Jeżeli osoba, której dane są przetwarzane zwróci się do Szpitala Specjalistycznego w Prabutach Sp. z o.o. z żądaniem potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz otrzymania informacji o przetwarzanych danych.
- 2) ADO zgodnie z art. 12 Rozporządzenia PE w komunikacji z osobą, której dane dotyczą stosuje się do zasad opisanych w pkt. 3.1.1 POD.
- 3) Zakres udzielanej informacji to zgodnie z art. 15 Rozporządzenia PE:
  - a) cele przetwarzania;
  - b) kategorie odnośnych danych osobowych;
  - c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych; Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, ADO informuje o odpowiednich zabezpieczeniach, o których mowa w art. 46 Rozporządzenia PE, związanych z przekazaniem;
  - d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
  - e) 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;
  - f) informacje o prawie wniesienia skargi do organu nadzorczego;
  - g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
  - h) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 Rozporządzenia PE, 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.
- 4) ADO dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, ADO może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.
- 5) Prawo do uzyskania kopii nie może niekorzystnie wpływać na prawa i wolności innych np. gdy uniemożliwia się stronom trzecim realizację ich praw jako osób, których dane dotyczą (praw do informacji, dostępu itd.). Jeżeli strony trzecie, których sprawa dotyczy, nie są informowane i nie mogą realizować swoich praw jako osoby, których dane dotyczą, wówczas istnieje prawdopodobieństwo, że takie przetwarzanie będzie niezgodne z prawem i nierzetelne. Tylko dane osobowe dotyczące osoby, której dane dotyczą, objęte są zakresem wniosku o dostęp do danych. W związku z tym wszelkie dane będące danymi anonimowymi



 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Lecznicy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
		Strona 43 z 81	
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

lub niedotyczące osoby, której dane dotyczą, nie będą wchodziły w ten zakres. Jednak dane poddane pseudonimizacji, które można wyraźnie powiązać z osobą, której dane dotyczą (np. poprzez podanie przez nią odnośnego identyfikatora, por. artykuł 11 ust. 2 Rozporządzenia PE), mieszczą się w tym zakresie. Jeżeli ADO przetwarza informacje, które zawierają dane osobowe kilku osób, których dane dotyczą, wówczas nie przyjmuje zbyt wąskiej interpretacji zdania „dane osobowe dane osobowe jej dotyczące”.

- 6) Prawa i wolności innych osób wskazane są w art. 20 ust. 4 Rozporządzenia PE mogą być rozumiane jako „obejmujące tajemnice handlowe lub własność intelektualną a w szczególności prawo autorskie chroniące oprogramowanie. Jednak mimo, że prawa te należy uwzględnić przed udzieleniem odpowiedzi na wniosek o przeniesienie danych, „skutkiem” tych rozważań nie powinna być odmowa zapewnienia osobie, której dane dotyczą, wszystkich informacji”. Ponadto prawo do dostępu nie jest prawem osoby do niewłaściwego wykorzystywania informacji w sposób, który można zaklasyfikować jako nierzetelną praktykę lub który stanowi naruszenie praw własności intelektualnej. Jednakże potencjalne ryzyko biznesowe nie może, samo w sobie, stanowić podstawy do odmowy udzielenia odpowiedzi na wniosek o udzielenie dostępu i ADO może przesłać dane osobowe przekazane przez osoby, których dane dotyczą, w formie, która nie ujawnia informacji objętych tajemnicą handlową lub prawami własności intelektualnej.
- 7) ADO odpowiednio uzasadnia i dokumentuje wszelkie decyzje odnośnie prawa do uzyskania kopii, które mogłyby niekorzystnie wpłynąć na prawa i wolności innych i jednocześnie stosuje się do zasad z pkt. 3.1.1. POD.



### **3.3. Prawo do sprostowania danych [16]**

- 1) Osoba, której dane dotyczą, ma prawo żądania od ADO niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.
- 2) ADO dokłada wszelkich starań, aby przetwarzane dane osobowe były prawidłowe i w razie potrzeby uaktualniane. ADO podejmuje wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane zgodnie z zasadą prawidłowości [5.1.d].
- 3) ADO zgodnie z art. 12 Rozporządzenia PE w komunikacji z osobą, której dane dotyczą stosuje się do zasad opisanych w pkt. 3.1.1. POD.
- 4) ADO informuje o sprostowaniu danych osobowych, których dokonał zgodnie z art. 16 Rozporządzenia PE, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. ADO informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda [19].

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
			Strona 44 z 81
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

### 3.4. Prawo do usunięcia danych („prawo do bycia zapomnianym”) [17]

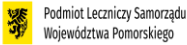
- 1) Osoba, której dane dotyczą, ma prawo żądania od ADO niezwłocznego usunięcia dotyczących jej danych osobowych, a ADO ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:
  - a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
  - b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) Rozporządzenia PE, i nie ma innej podstawy prawnej przetwarzania;
  - c) osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 Rozporządzenia PE wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 Rozporządzenia PE wobec przetwarzania;
  - d) dane osobowe były przetwarzane niezgodnie z prawem;
  - e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega ADO;
  - f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku, na podstawie zgody osoby, której dane dotyczą, na przetwarzanie swoich danych osobowych w jednym, lub większej liczbie określonych celów (zgodne z prawem jest przetwarzanie danych osobowych dziecka, które ukończyło 16 lat; jeżeli dziecko nie ukończyło 16 lat, takie przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy zgodę wyraziła lub zaaprobowała ją osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody).
- 2) ADO informuje o usunięciu danych osobowych, których dokonał zgodnie z art. 17 ust. 1 Rozporządzenia PE, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. ADO informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda [19].
- 3) W przypadku, gdy ADO upublicznił dane osobowe, a ma obowiązek usunąć te dane osobowe zgodnie z wytycznymi powyżej (art. 17 ust. 1 Rozporządzenia PE), 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.
- 4) ADO zgodnie z art. 12 Rozporządzenia PE w komunikacji z osobą, której dane dotyczą stosuje się do zasad opisanych w pkt. 3.1.1 POD.

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
			Strona 45 z 81
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

- 5) ADO zobowiązany jest do usunięcia danych, które były przetwarzane na podstawie zgody, gdy zgoda zostaje wycofana, to osoba, której dane dotyczą, ma również możliwość zażądania usunięcia innych dotyczących jej danych, które nadal znajdują się u ADO, np. na podstawie art. 6 ust. 1b Rozporządzenia PE. W tym celu osoba, której dane dotyczą, może skorzystać z prawa do usunięcia danych, zgodnie z art. 17 ust. 1 pkt. b Rozporządzenia PE i motywem 65 zawartych w Rozporządzeniu PE. Wówczas ADO dokonuje oceny, czy dalsze przetwarzanie danych wskazanych powyżej jest właściwe, nawet w przypadku braku żądania usunięcia danych przez osobę, której dane dotyczą.
- 6) ADO nie ma obowiązku usunąć danych osobowych w zakresie w jakim przetwarzanie jest niezbędne:
- a) do korzystania z prawa do wolności wypowiedzi i informacji;
  - b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega ADO, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej ADO;
  - c) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3 Rozporządzenia PE;
  - d) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 Rozporządzenia PE, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania;
  - e) lub do ustalenia, dochodzenia lub obrony roszczeń.

### **3.5. Prawo do ograniczenia przetwarzania [18]**


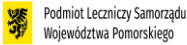
- 1) Osoba, której dane dotyczą, ma prawo żądania od ADO ograniczenia przetwarzania w następujących przypadkach:
- a) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający ADO sprawdzić prawidłowość tych danych;
  - b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
  - c) ADO nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
  - d) osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 Rozporządzenia PE wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie ADO są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.
- 2) Jeżeli ADO ograniczył przetwarzanie zgodnie z ust. 1 wówczas takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, tylko wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

<p>Szpital Specjalistyczny w Prabutach sp. z o.o.</p> 	PROCEDURA	Wydanie: 3	<b>10.08.2025</b>
		Strona 46 z 81	
	POLITYKA OCHRONY DANYCH OSOBOWYCH	Nr dokumentu: <b>7- Pr5</b>	



- 3) Przed uchyleniem ograniczenia przetwarzania ADO informuje o tym osobę, której dane dotyczą, a która żądała ograniczenia zgodnie z ust. 1.
- 4) Wśród metod pozwalających ograniczyć przetwarzanie danych osobowych mogą się znaleźć między innymi: czasowe przeniesienie wybranych danych osobowych do innego systemu przetwarzania, uniemożliwienie użytkownikom dostępu do wybranych danych, lub czasowe usunięcie opublikowanych danych ze strony internetowej. W zautomatyzowanych zbiorach danych przetwarzanie należy zasadniczo ograniczyć środkami technicznymi w taki sposób, by dane osobowe nie podlegały dalszemu przetwarzaniu ani nie mogły być zmieniane. Fakt ograniczenia przetwarzania danych osobowych należy wyraźnie zaznaczyć w systemie.
- 5) ADO zgodnie z art. 12 Rozporządzenia PE w komunikacji z osobą, której dane dotyczą stosuje się do zasad opisanych w pkt. 3.1.1 POD.
- 6) ADO informuje o ograniczeniu przetwarzania danych osobowych, których dokonał zgodnie z art. 18 Rozporządzenia PE, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. ADO informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda [19].

### 3.6. Prawo do przenoszenia danych [20]

- 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 jeżeli:
  - a) przetwarzanie odbywa się na podstawie zgody w myśl art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) Rozporządzenia PE lub na podstawie umowy w myśl art. 6 ust. 1 lit. b) Rozporządzenia PE; oraz
  - b) przetwarzanie odbywa się w sposób zautomatyzowany.
- 2) Rozporządzenie PE nie ustanawia ogólnego prawa do przenoszenia danych dla przypadków, w których przetwarzanie danych osobowych nie odbywa się na podstawie zgody lub umowy. Jeżeli chodzi o dane pracowników, prawo do przenoszenia danych ma generalnie zastosowanie tylko, jeżeli przetwarzanie jest oparte na umowie, której stroną jest osoba, której dane dotyczą. W wielu przypadkach zgoda nie będzie uznana za dobrowolnie wyrażoną w tym kontekście, ze względu na brak równowagi sił między pracodawcą a pracownikiem. Natomiast niektóre operacje przetwarzania w kontekście HR (zasobów ludzkich) oparte są na podstawie prawnej prawnie uzasadnionego interesu lub są konieczne do zapewnienia przestrzegania określonych zobowiązań prawnych w obszarze zatrudnienia. W praktyce prawo do przenoszenia danych w kontekście HR niewątpliwie dotyczyć będzie określonych operacji przetwarzania (takich jak usługi w zakresie płac i wynagrodzeń, wewnętrzna rekrutacja), ale w wielu sytuacjach potrzebne będzie podejście dla poszczególnych przypadków, wówczas ADO weryfikuje, czy spełnione są wszystkie warunki mające zastosowanie do prawa do przenoszenia danych.


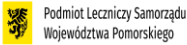
 Szpital Specjalistyczny w Prabutach sp. z o.o.	PROCEDURA	Wydanie: 3	<b>10.08.2025</b>
		Strona 47 z 81	
 Podmiot Lecznicy Samorządu Województwa Pomorskiego	POLITYKA OCHRONY DANYCH OSOBOWYCH	Nr dokumentu: <b>7- Pr5</b>	

- 3) Prawo do przenoszenia danych ma zastosowanie tylko, jeżeli przetwarzanie danych „odbywa się w sposób zautomatyzowany”, i w związku z tym nie obejmuje większości zbiorów papierowych.
- 4) ADO ułatwia wykonywanie prawa do przenoszenia danych przez osobę, której dane dotyczą.
- 5) Prawo do przenoszenia nie może być naruszane ani ograniczone do danych osobowych bezpośrednio przekazanych przez osobę, której dane dotyczą, na przykład w formularzu online.
- 6) Prawo do przenoszenia danych nie jest ograniczone do danych osobowych, które są przydatne i istotne dla podobnych usług świadczonych przez konkurencję ADO.
- 7) Podstawowym celem przenoszenia danych jest zwiększenie kontroli osoby nad jej danymi osobowymi oraz zapewnienie odgrywania przez nie czynnej roli w ekosystemie danych. Artykuł 20 Rozporządzenia PE nie ogranicza danych podlegających przenoszeniu tylko do tych, które są konieczne lub przydatne do zmiany usługi.
- 8) ADO zgodnie z art. 12 Rozporządzenia PE w komunikacji z osobą, której dane dotyczą stosuje się do zasad opisanych w pkt. 3.1.1 POD.
- 9) ADO zwraca szczególną uwagę na format danych, które mają być przesłane, aby zagwarantować, że dane będą mogły być ponownie wykorzystane, z małym wysiłkiem, przez osobę, której dane dotyczą, lub innego administratora danych.
- 10) Dane osobowe muszą być przekazane „w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego”. Format ten powinien być interoperacyjny, który to termin definiowany jest w UE jako: możliwość współdziałania różnych odrębnych organizacji na rzecz osiągnięcia uzgodnionych i korzystnych dla wszystkich stron celów, przy jednoczesnym dzieleniu się informacjami i wiedzą pomiędzy tymi organizacjami poprzez wspierane przez nie procesy biznesowe, za pomocą wymiany danych za pośrednictwem odpowiednich systemów TIK. Terminy „ustrukturyzowany”, „powszechnie używany” oraz „nadający się do odczytu maszynowego” stanowią zestaw minimalnych wymogów, które powinny umożliwiać interoperacyjność danych przekazanych przez administratora danych. Odpowiednie formaty ADO wybiera tak, aby osiągnąć cel bycia interpretowalnym i zapewnić osobie, której dane dotyczą, duży stopień przenoszenia danych. ADO nie wybiera formatów podlegających ograniczeniom w zakresie kosztownych licencji. ADO wcześniej identyfikuje dane wchodzące w zakres przenoszenia w jego własnym systemie. To dodatkowe przetwarzanie danych będzie uznawane za element dodatkowy głównego przetwarzania danych, ponieważ nie jest ono dokonywane w celu osiągnięcia nowego celu określonego przez ADO. ADO przekazuje dane osobowe przy użyciu powszechnie wykorzystywanych formatów (np. XML, JSON, CSV, ...) wraz z przydatnymi metadanymi na najlepszym poziomie szczegółowości, przy jednoczesnym zachowaniu wysokiego poziomu abstrakcji. Jako, takie, odpowiednie metadane powinny być wykorzystane w celu prawidłowego opisanie znaczenia informacji będących przedmiotem wymiany. Te metadane powinny być wystarczające do umożliwienia funkcjonowania

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	PROCEDURA	Wydanie: 3	<b>10.08.2025</b>
			Strona 48 z 81
	POLITYKA OCHRONY DANYCH OSOBOWYCH	Nr dokumentu: <b>7- Pr5</b>	

i ponownego wykorzystywania danych, ale oczywiście bez ujawniania tajemnicy handlowej. ADO uwzględnia, jak format danych może wpłynąć na prawo osoby do ponownego wykorzystywania danych lub jak może to prawo ograniczyć. W przypadkach gdy ADO może zapewnić osobie, której dane dotyczą, możliwość wyboru preferowanego formatu danych osobowych, wówczas zapewnia zrozumiałe wyjaśnienie dotyczące skutku (wpływu), jaki będzie miał określony wybór. Jednak ADO uwzględnia, że przetwarzanie dodatkowych metadanych tylko dla celu, że mogłyby być potrzebne do udzielenia odpowiedzi na wniosek o przeniesienie danych, nie stwarza podstawy prawnej do takiego przetwarzania.

- 11) W przypadku dużego zbioru danych, złożonej struktury danych lub innych kwestii technicznych, które mogą stwarzać trudności ADO lub osobom, których dane dotyczą, kluczowe jest, aby osoba była w stanie całkowicie zrozumieć definicję, schemat i strukturę danych osobowych, które mogą być przekazywane przez ADO. Na przykład dane mogą najpierw być przekazane w skróconej zorganizowanej formie pozwalającej osobie, której dane dotyczą, na przenoszenie raczej części (podzbiorów) danych osobowych, a nie całości. ADO przedstawia przegląd „w zwartej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem” najlepiej w taki sposób, aby osoba, której dane dotyczą, zawsze miała jasne informacje na temat tego, jakie dane pobrać lub przesłać innemu administratorowi danych w związku z określonym celem.
- 12) Osoba, której dane dotyczą, ma prawo do otrzymania podzbioru danych osobowych jej dotyczących przetwarzanych przez ADO oraz przechowywania tych danych w celu dalszego osobistego wykorzystania. Tego typu przechowanie może mieć miejsce na urządzeniu prywatnym lub w prywatnej chmurze, bez konieczności przesyłania ich innemu administratorowi danych.
- 13) Osoba, której dane dotyczą, wnioskująca o dane jest odpowiedzialna za znalezienie właściwych środków w celu zabezpieczenia danych osobowych we własnym systemie. Jednak ADO informuje ją o tym fakcie, aby mogła podjąć kroki na rzecz ochrony informacji, które otrzymała. ADO może również zalecić odpowiedni format(y), narzędzia do szyfrowania i inne środki bezpieczeństwa, aby pomóc osobie, której dane dotyczą, w osiągnięciu tego celu.
- 14) Osoba, której dane dotyczą, ma prawo przesłać w/w otrzymane dane osobowe innemu administratorowi bez przeszkód ze strony ADO (któremu dostarczono te dane osobowe).
- 15) W przypadku, gdy osoba, której dotyczą dane osobowe, złoży żądanie by jej dane osobowe zostały przesłane przez ADO bezpośrednio innemu administratorowi, wówczas ADO o ile jest to technicznie możliwe, dołoży możliwych starań, aby tak się stało zgodnie z art. 20 ust. 2 Rozporządzenia PE.
- 16) Bezpośrednie przesłanie danych w interoperacyjnym formacie przez ADO do innego administratora i od innego administratora do ADO, może mieć miejsce, gdy możliwa jest komunikacja między dwoma systemami, w zabezpieczony sposób, oraz gdy system otrzymujący ma techniczną możliwość otrzymania przychodzących danych. Jeżeli przeszkody techniczne uniemożliwiają bezpośrednie przekazanie, ADO wyjaśnia osobom,


 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	PROCEDURA	Wydanie: 3	10.08.2025
		Strona 49 z 81	
	POLITYKA OCHRONY DANYCH OSOBOWYCH	Nr dokumentu: <b>7- Pr5</b>	

których dane dotyczą, kwestię tych przeszkód, ponieważ w przeciwnym razie jego decyzja będzie miała podobny skutek jak odmówienie podjęcia działań na żądanie osoby, której dane dotyczą (art. 12 ust. 4 Rozporządzenia PE). Na poziomie technicznym administratorzy danych powinni zbadać i ocenić dwa różne i uzupełniające się sposoby udostępniania danych podlegających przenoszeniu osobom, których dane dotyczą, lub innym administratorom danych:

- bezpośrednie przekazanie całego zbioru danych zawierającego dane podlegające przenoszeniu (lub kilka fragmentów z części globalnego zbioru danych);
- zautomatyzowane narzędzie umożliwiające pobieranie istotnych danych.



Te dwa różne i potencjalnie uzupełniające się sposoby przekazywania istotnych danych podlegających przenoszeniu można wdrożyć, udostępniając dane przy użyciu różnych środków, takich jak np. bezpieczna wymiana komunikatów, serwer SFTP, zabezpieczony interfejs komunikacyjny WebAPI lub portal internetowy. Należy umożliwić osobom, których dane dotyczą, korzystanie z bazy danych osobowych, systemu zarządzania danymi osobowymi lub innych rodzajów rozwiązań zaufanych stron trzecich, w celu przechowywania danych osobowych i udzielania administratorom danych pozwoleń na dostęp i przetwarzanie danych osobowych, gdy jest takie żądanie.

- 17) ADO jest odpowiedzialny za podjęcie wszelkich środków bezpieczeństwa potrzebnych do zapewnienia nie tylko, aby dane osobowe zostały bezpiecznie przesłane (np. z zastosowaniem szyfrowania na całej drodze przesyłu danych lub szyfrowania danych) do właściwego miejsca przeznaczenia (przy użyciu silnych środków uwierzytelniających), ale także kontynuując ochronę danych osobowych, które pozostają w ich systemach, jak również przejrzyste procedury postępowania z możliwymi naruszeniami danych. W takiej sytuacji ADO ocenia określone zagrożenia związane z przenoszeniem danych i podejmuje odpowiednie środki ograniczające ryzyko. Takie środki ograniczające ryzyko mogą obejmować: jeżeli osoba, której dane dotyczą, już musi być uwierzytelniona, wykorzystanie dodatkowych informacji uwierzytelniających, takich jak wspólna tajemnica, lub inny czynnik uwierzytelnienia, taki jak jednorazowe hasło; zawieszenie przesyłania, jeżeli istnieje podejrzenie, że doszło do naruszenia konta; w przypadkach bezpośredniego przesyłania od jednego administratora danych do innego administratora danych, powinny być stosowane uwierzytelnienia z polecenia, np. uwierzytelnienie oparte na tokenie. Takie środki bezpieczeństwa nie mogą stanowić przeszkody ani nie mogą uniemożliwiać użytkownikom realizacji ich praw, np. poprzez nałożenie dodatkowych kosztów. Bowiem zgodnie z art. 5 ust 1 pkt. f Rozporządzenia PE to ADO powinien zagwarantować „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.
- 18) ADO odpowiadając na wniosek o przeniesienie danych, na warunkach określonych w art. 20 Rozporządzenia PE, nie jest odpowiedzialny za przetwarzanie prowadzone przez osobę, której dane dotyczą, lub przez inne przedsiębiorstwo otrzymujące dane osobowe. ADO

<p>Szpital Specjalistyczny w Prabutach sp. z o.o.</p>  <p>Podmiot Leczniczy Samorządu Województwa Pomorskiego</p>	<p>PROCEDURA</p>	Wydanie: 3	10.08.2025
		Strona 50 z 81	
	<p>POLITYKA OCHRONY DANYCH OSOBOWYCH</p>	Nr dokumentu: <b>7- Pr5</b>	


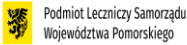
działa w imieniu osoby, której dane dotyczą, w tym gdy dane osobowe są przesyłane bezpośrednio do innego administratora danych. W tym zakresie ADO nie jest odpowiedzialny za zapewnienie zgodności z prawem ochrony danych przez otrzymującego administratora danych, zważywszy że wysyłający administrator danych nie wybiera odbiorcy.

- 19) ADO ustanawia zabezpieczenia w celu zapewnienia, że będzie rzeczywiście działać w imieniu osoby, której dane dotyczą.
- 20) Aby zapewnić, że przesyłane dane osobowe rzeczywiście będą danymi, które osoba, której dane dotyczą, chce przesłać, ADO uzyskuje potwierdzenie od osoby, której dane dotyczą albo przed przesłaniem albo wcześniej, gdy udzielana jest pierwotna zgoda na przetwarzanie lub gdy finalizowana jest umowa.
- 21) ADO odpowiadając na wniosek o przeniesienie danych nie ma określonego obowiązku sprawdzenia i weryfikacji jakości danych przed ich przesłaniem, jednak dane te powinny już być prawidłowe oraz aktualne, zgodnie z zasadami określonym w artykule 5 ust. 1 Rozporządzenia PE.
- 22) Po operacji przeniesienia danych, osoba, której dane dotyczą, może nadal korzystać z usług ADO, bowiem przenoszenie danych nie powoduje automatycznie usunięcia danych z systemów ADO i nie wpływa na pierwotny okres przechowywania mający zastosowanie wobec danych, które zostały przesłane. Osoba, której dane dotyczą, może realizować swoje prawa, o ile ADO nadal przetwarza dane.
- 23) Prawo do przenoszenia danych nie nakłada na ADO obowiązku zatrzymywania danych osobowych dłużej niż to konieczne, czy też dłużej niż przez określony okres przechowywania. Nie ma dodatkowego wymogu zatrzymywania danych w okresach innych niż te mające zastosowanie, po prostu w celu realizacji potencjalnego przyszłego wniosku o przeniesienie danych.
- 24) ADO może zdecydować o przyjęciu danych od osoby, której dane dotyczą, ale nie jest do tego zobowiązany.
- 25) ADO jako „otrzymujący” administrator danych, zapewnia osobom, których dane dotyczą, kompletne informacje na temat charakteru danych osobowych, które są istotne dla realizacji jego usług.
- 26) Jeżeli ADO otrzymuje dane wówczas staje się nowym administratorem danych w odniesieniu do tych danych osobowych, wówczas wyraźnie i bezpośrednio określa cel nowego przetwarzania przed jakimkolwiek wnioskiem o przesłanie danych podlegających przenoszeniu, zgodnie z wymogami przejrzystości określonymi w art. 14 Rozporządzenia PE.
- 27) Jako nowy administrator ADO przestrzega zasad określonych w art. 5 Rozporządzenia PE, takich jak zgodność z prawem, rzetelność i przejrzystość, ograniczenie celu, minimalizacja danych, prawidłowość, integralność i poufność, ograniczenie przechowywania i rozliczalność. Jeżeli ADO otrzymuje dane wówczas jest odpowiedzialny za zapewnienie, aby przekazane dane podlegające przenoszeniu były stosowne i nie nadmierne

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	PROCEDURA	Wydanie: 3	<b>10.08.2025</b>
			Strona 51 z 81
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

w odniesieniu do nowego przetwarzania danych. Przyjęte i zatrzymane dane powinny obejmować tylko te dane, które są niezbędne i istotne dla usługi świadczonej przez ADO jako administratora otrzymującego dane.

- 28) ADO jako nowy administrator danych nie przetwarza danych osobowych, które nie są stosowne, a przetwarzanie jest ograniczone do tego, co jest niezbędne do nowych celów, nawet jeśli dane osobowe stanowią część bardziej globalnego zestawu danych przesyłanego w ramach procedury przenoszenia. Dane osobowe, które nie są niezbędne do osiągnięcia celu nowego przetwarzania, ADO usuwa tak szybko jak to możliwe.
- 29) Prawo do przenoszenia danych, nie może niekorzystnie wpływać na prawa i wolności innych. Na przykład rejestry połączeń telefonicznych, wiadomości interpersonalnych lub VoIP [usług telefonii internetowej] (w historii konta abonenta) mogą zawierać dane stron trzecich zaangażowanych w połączenia przychodzące i wychodzące. Mimo, że rejestry będą w związku z tym zawierały dane osobowe dotyczące wielu osób, abonenci powinni mieć możliwość otrzymania tych rejestrów w odpowiedzi na wnioski o przenoszenie danych, ponieważ rejestry dotyczą (także) osoby, której dane dotyczą. Jednak, gdy takie rejestry są następnie przesyłane nowemu administratorowi danych, ten nowy administrator danych nie powinien ich przetwarzać w żadnym celu, który by negatywnie wpłynął na prawa i wolności stron trzecich (m.in. na realizację praw, jako osób, których dane dotyczą na mocy Rozporządzenia PE). Osoba, której dane dotyczą, inicjująca przesyłanie jej danych innemu administratorowi danych, albo wyraża zgodę na przetwarzanie danych przez nowego administratora danych albo zawiera umowę z tym administratorem. Gdy dane osobowe stron trzecich zawarte są w zbiorze danych, należy określić inną podstawę prawną przetwarzania. Na przykład prawnie uzasadniony interes może być realizowany przez ADO na mocy artykułu 6 ust. 1 lit. f) Rozporządzenia PE, w szczególności gdy celem ADO jest świadczenie usługi osobie, której dane dotyczą, co pozwala tej ostatniej przetwarzać dane osobowe w ramach czynności o czysto osobistym lub domowym charakterze. Operacje przetwarzania zainicjowane przez osobę, której dane dotyczą, w kontekście czynności o osobistym charakterze, które dotyczą i mają potencjalny wpływ na strony trzecie, pozostają w zakresie jej odpowiedzialności, w stopniu, w jakim o takim przetwarzaniu, w żaden sposób, nie decyduje ADO.
- 30) ADO jako otrzymujący „nowy” administrator danych (któremu dane mogą być przesłane na wniosek użytkownika) nie wykorzystuje przesłanych danych stron trzecich do własnych celów. Przetwarzanie takich danych osobowych jest dozwolone tylko w zakresie, w jakim dane są przechowywane pod wyłączną kontrolą wnioskującego użytkownika i są przetwarzane tylko na potrzeby o czysto osobistym lub domowym charakterze. Informacje te nie będą również wykorzystane do uzyskania informacji na temat takich stron trzecich oraz tworzenia określonych profili, nawet jeżeli ich dane osobowe już są w posiadaniu ADO.
- 31) Prawa i wolności innych osób wskazane są w artykule 20 ust. 4 Rozporządzenia PE, podczas gdy nie są bezpośrednio związane z przenoszeniem, mogą być rozumiane jako „obejmujące tajemnice handlowe lub własność intelektualną a w szczególności prawo



 Szpital Specjalistyczny w Prabutach sp. z o.o.	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
		Strona 52 z 81	
 Podmiot Leczniczy Samorządu Województwa Pomorskiego	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

autorskie chroniące oprogramowanie. Jednak mimo że prawa te należy uwzględnić przed udzieleniem odpowiedzi na wniosek o przeniesienie danych, „skutkiem” tych rozważań nie powinna być odmowa zapewnienia osobie, której dane dotyczą, wszystkich informacji”. Ponadto prawo do przenoszenia danych nie jest prawem osoby do niewłaściwego wykorzystywania informacji w sposób, który można zaklasyfikować jako nierzetelną praktykę lub który stanowi naruszenie praw własności intelektualnej. ADO przesyła dane osobowe przekazane przez osoby, których dane dotyczą, w formie, która nie ujawnia informacji objętych tajemnicą handlową lub prawami własności intelektualnej, gdyż potencjalne ryzyko biznesowe nie może, samo w sobie, stanowić podstawy do odmowy udzielenia odpowiedzi na wniosek o przeniesienie.



- 32) Wykonanie prawa do przenoszenia danych, pozostaje bez uszczerbku dla art. 17 Rozporządzenia PE - Prawa do usunięcia danych („prawa do bycia zapomnianym”). Jeżeli osoba, której dane dotyczą, chce zrealizować swoje prawo do usunięcia danych „prawa do bycia zapomnianym” na mocy art. 17 Rozporządzenia PE, przenoszenie danych nie może być zastosowane przez administratora danych jako sposób opóźnienia lub odmowy takiego usunięcia. Jeżeli osoba, której dane dotyczą, dowie się, że dane osobowe wnioskowane na mocy prawa do przenoszenia danych nie odpowiadają w pełni jej wnioskowi, każdy kolejny wniosek o dostęp do danych osobowych na mocy prawa dostępu winien być w pełni zrealizowany, zgodnie z art. 15 Rozporządzenia PE. Ponadto w przypadku, gdy szczególne prawo europejskie lub prawo państwa członkowskiego w innym obszarze również przewiduje jakąś formę przenoszenia przedmiotowych danych, warunki określone w takim prawie szczególnym także muszą być wzięte pod uwagę przy realizacji wniosku o przeniesienie danych na mocy Rozporządzenia PE. Po pierwsze, jeżeli z wniosku złożonego przez osobę, której dane dotyczą, wyraźnie wynika, że jej zamiarem nie jest realizacja praw na mocy Rozporządzenia PE, ale raczej realizacja praw na mocy tylko ustawodawstwa sektorowego, przepisy Rozporządzenia PE dotyczące przenoszenia danych nie będą miały zastosowania do tego wniosku. Jeżeli, z drugiej strony, celem wniosku jest przeniesienie na mocy Rozporządzenia PE, istnienie takiego szczególnego ustawodawstwa nie uchyla zastosowania zasady przenoszenia danych wobec każdego administratora danych, jak przewidziano w Rozporządzeniu PE. ADO wówczas ocenia, dla poszczególnych przypadków, jak, o ile w ogóle, takie szczególne ustawodawstwo może wpłynąć na prawo do przenoszenia danych.
- 33) Prawo do przenoszenia danych nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej ADO. W związku z tym w tych przypadkach ADO nie ma obowiązku zapewniania przenoszenia danych. Jednak odpowiadania na wnioski o przeniesienie, z poszanowaniem zasad regulujących prawo do przenoszenia danych.

### **3.7. Prawo do sprzeciwu [21]**

- 1) Wobec przetwarzania opartego na art. 6 ust. 1 lit. e) lub f) Rozporządzenia PE:

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
			Strona 53 z 81
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	



- a) 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) Rozporządzenia PE, w tym profilowania na podstawie tych przepisów.
  - b) ADO nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.
  - c) ADO przygotowuje Opinię w celu wykazania i udokumentowania istnienia ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.
  - d) Jeżeli istnieją ważne prawnie uzasadnione podstawy przetwarzania, nadrzędne wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń, wówczas ADO sprawdza, czy te ważne prawnie uzasadnione podstawy przetwarzania i ich cele są zbieżne z celami i podstawami prawnymi przetwarzania, którego dokonywano przed złożeniem sprzeciwu wobec przetwarzania przez osobę, której dane dotyczą.
  - e) Jeżeli ze sprawdzenia, dokonanego zgodnie z punktem powyżej, wynika, że dane osoby, która złożyła sprzeciw, będą przetwarzane na innej niż dotychczas podstawie przetwarzania lub w innym celu, wówczas ADO spełnia obowiązek informacyjny [13-14] wobec tej osoby.
- 2) Wobec przetwarzania na potrzeby marketingu bezpośredniego:
    - a) 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 tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.
    - b) Jeżeli osoba, której dane dotyczą, wnieśli sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów.
  - 3) Najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie, o którym mowa w art. 21 ust. 1 i 2 Rozporządzenia PE, oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji (3.1.2 POD).
  - 4) Osoba, której dane dotyczą, może wykonać prawo do sprzeciwu za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne.
  - 5) ADO zgodnie z art. 12 Rozporządzenia PE w komunikacji z osobą, której dane dotyczą stosuje się do zasad opisanych w pkt. 3.1.1 POD.
  - 6) Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 Rozporządzenia PE, osoba, której dane dotyczą,

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
			Strona 54 z 81
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	



ma prawo wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

### **3.8. Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie [22]**

- 1) Zgodnie z art. 2 ust. 1 Rozporządzenia PE, rozporządzenie to ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych. W związku z powyższym ochrona danych osobowych ma zastosowanie do zautomatyzowanego przetwarzania danych osobowych oraz do przetwarzania ręcznego, jeżeli dane osobowe znajdują się lub mają się znaleźć w zbiorze danych. Zbiory lub zestawy zbiorów oraz ich strony tytułowe, które nie są uporządkowane według określonych kryteriów nie są objęte zakresem Rozporządzenia PE.
- 2) 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, gdzie:
  - a) zautomatyzowane przetwarzanie danych to operacja lub zestaw operacji na danych, takie jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie, wykonywanych w systemach informatycznych (gdzie system informatyczny to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych),
  - b) zautomatyzowanym podejmowaniem decyzji jest proces, w wyniku którego decyzja zostaje wydana bez ludzkiej ingerencji w jej podejmowanie; za jego przykład można podać automatyczne odrzucenie elektronicznego wniosku kredytowego czy elektroniczne metody rekrutacji bez interwencji ludzkiej,
  - c) profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.
- 3) Ust. 2 nie ma zastosowania, jeżeli ta decyzja:
  - a) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem;

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
			Strona 55 z 81
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

- b) jest dozwolona prawem Unii 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.
- 4) W przypadkach, o których mowa w ust. 3 lit. a) i c), administrator wdraża właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji.
- 5) Decyzje, o których mowa w ust. 3, nie mogą opierać się na szczególnych kategoriach danych osobowych, o których mowa w art. 9 ust. 1 Rozporządzenia PE, chyba że zastosowanie ma art. 9 ust. 2 lit. a) lub g) Rozporządzenia PE i istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.
- 6) ADO zgodnie z art. 12 Rozporządzenia PE w komunikacji z osobą, której dane dotyczą stosuje się do zasad opisanych w pkt. 3.1.1 POD.
- 7) ADO nie podejmuje decyzji, które opierałyby się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu.

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Lecznicy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
			Strona 56 z 81
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

## 4. Naruszenia ochrony danych osobowych [33 i 34]

### 1) Procedura zgłaszania naruszeń do organu nadzorczego[33]:

W przypadku naruszenia ochrony danych osobowych, ADO zgłasza takie naruszenie do Prezesa Urzędu Ochrony Danych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Zgłaszanie naruszeń do Prezesa Urzędu Ochrony Danych następuje bez zbędnej zwłoki – w miarę możliwości, nie później jednak niż w terminie 72 godzin od stwierdzenia naruszenia.

Zgłoszenie, zgodnie z wytycznymi z art. 33 ust. 3 Rozporządzenia PE, musi co najmniej:

- a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
- b) zawierać imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
- d) opisywać środki zastosowane lub proponowane przez ADO w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.


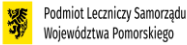
Jeżeli nie wszystkie wymagane informacje dotyczące naruszenia są dostępne od razu, wówczas dopuszczalne jest ich bezzwłoczne, sukcesywne podawanie. Niemniej jeżeli samo zgłoszenie nastąpi już po upływie 72 godzin, to ADO dołącza do niego wyjaśnienie przyczyny opóźnienia.

ADO dokumentuje, zgodnie z zasadą rozliczalności, w sposób przejrzysty i umożliwiający Prezesowi Urzędu Ochrony Danych weryfikowanie przestrzegania art. 33 Rozporządzenia PE, wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutków oraz podjętych działań zaradczych.

### 2) Procedura zgłaszania naruszeń do osoby, której dane dotyczą [34]:

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, ADO bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu, tak aby umożliwić jej podjęcie niezbędnych działań zapobiegawczych [34.1].

Powyższe zawiadomienie jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki o których mowa w art. 33 ust. 3 lit. b), c) i d) Rozporządzenia PE:

 Szpital Specjalistyczny w Prabutach sp. z o.o.	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
		Strona 57 z 81	
 Podmiot Lecznicy Samorządu Województwa Pomorskiego	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

- a) zawiera imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- b) opisuje możliwe konsekwencje naruszenia ochrony danych osobowych;
- c) opisuje środki zastosowane lub proponowane przez ADO w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

ADO zgodnie z art. 12 Rozporządzenia PE w komunikacji z osobą, której dane dotyczą stosuje się do zasad opisanych w pkt. 3.1.1 POD.

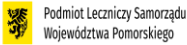
Powyższe zawiadomienie nie jest wymagane jeżeli:

- a) ADO wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiający odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
- b) ADO zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
- c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku ADO wydaje publiczny komunikat lub stosuje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skutecznym sposób [34].

Jeżeli ADO nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, organ nadzorczy – biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko – może od niego tego zażądać lub może stwierdzić, że spełniony został jeden z warunków, o których mowa powyżej (art. 34 ust. 4 Rozporządzenia PE).



## **5. Ocena skutków dla ochrony danych [35]**

- 1) ADO przeprowadza ocenę skutków dla ochrony danych obowiązkowo:
  - a) w szczególności w przypadku „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,
  - b) gdy przetwarzane mają być na dużą skalę szczególne kategorie danych osobowych lub dane dotyczące wyroków skazujących i naruszeń prawa,
  - c) gdy systematycznie monitorowane są na dużą skalę miejsca dostępne publicznie (art. 35 ust. 3 Rozporządzenia PE),
  - d) w przypadku, gdy dany rodzaj operacji przetwarzania został podany w wykazie operacji podlegających wymogowi dokonania oceny skutków dla ochrony danych publikowanym przez organ nadzorczy.

<p>Szpital Specjalistyczny w Prabutach sp. z o.o.</p> 	<p>PROCEDURA</p>	Wydanie: 3	10.08.2025
		Strona 58 z 81	
	<p>POLITYKA OCHRONY DANYCH OSOBOWYCH</p>	Nr dokumentu: <b>7- Pr5</b>	

- 2) 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, ADO przed rozpoczęciem przetwarzania dokonuje oceny skutków dla ochrony danych, która zawiera co najmniej:
  - a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;
  - b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
  - c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w art. 35 ust. 1 Rozporządzenia PE;
  - d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie Rozporządzenia PE, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.
- 3) Obowiązek przeprowadzenia takiej oceny, by przed przetwarzaniem danych ocenić jego skutki dla ochrony danych, źródła ryzyka oraz konkretne prawdopodobieństwo i wagę ryzyka, uwzględniając charakter, zakres, kontekst i cele przetwarzania, nie jest traktowany jako jednorazowa czynność, lecz raczej jako szerszy proces wymagający podejmowania w razie konieczności dalszych czynności, gdy zmieniają się ryzyka związane z operacjami przetwarzania danych osobowych.
- 4) Dokonując oceny skutków dla ochrony danych, administrator konsultuje się z IOD, jeżeli został on wyznaczony. ADO konsultuje z IOD m.in. następujące kwestie:
  - a) fakt, czy należy przeprowadzić ocenę skutków dla ochrony danych,
  - b) metodologię przeprowadzenia oceny skutków dla ochrony danych,
  - c) fakt, czy należy przeprowadzić wewnętrzną ocenę skutków dla ochrony danych czy też zlecić ją podmiotowi zewnętrznemu,
  - d) zabezpieczenia (w tym środków technicznych i organizacyjnych) stosowanych do łagodzenia wszelkich zagrożeń praw i interesów osób, których dane dotyczą,
  - e) prawidłowość przeprowadzonej oceny skutków dla ochrony danych i zgodność jej wyników z wymogami ochrony danych (czy należy kontynuować przetwarzanie czy też nie oraz jakie zabezpieczenia należy zastosować).

Jeśli administrator nie zgadza się z zaleceniami IOD, dokumentacja oceny skutków dla ochrony danych zawiera pisemne uzasadnienie nieuwzględnienia tych zaleceń.
- 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 lub bezpieczeństwa operacji przetwarzania.
- 6) Jeżeli przetwarzanie na mocy:

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
			Strona 59 z 81
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	



- art. 6 ust. 1 lit. c) Rozporządzenia PE: przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na ADO,
- lub art. 6 ust. 1 lit. e) Rozporządzenia PE: przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej ADO,

ma podstawę prawną w prawie Unii lub w prawie państwa członkowskiego, któremu podlega ADO, i prawo takie reguluje daną operację przetwarzania lub zestaw operacji, a oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej, wówczas art. 35 ust. 1-7 nie mają zastosowania, chyba że państwa członkowskie uznają za niezbędne, by przed podjęciem czynności przetwarzania dokonać oceny skutków dla ochrony danych.

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

## 6. Uprzednie Konsultacje [36]

- 1) Jeżeli ocena skutków dla ochrony danych, o której mowa w art. 35 Rozporządzenia PE, wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby ADO nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania ADO konsultuje się z organem nadzorczym.
- 2) Jeżeli organ nadzorczy jest zdania, że zamierzone przetwarzanie, o którym mowa w ust. 1, stanowiłoby naruszenie Rozporządzenia PE – w szczególności gdy ADO niedostatecznie zidentyfikował lub zminimalizował ryzyko – organ nadzorczy w terminie do ośmiu tygodni od wpłynięcia wniosku o konsultacje udziela ADO, a gdy ma to zastosowanie także podmiotowi przetwarzającemu pisemnego zalecenia i może skorzystać z dowolnego ze swoich uprawnień, o których mowa w art. 58 Rozporządzenia PE. Okres ten można przedłużyć o sześć tygodni ze względu na złożony charakter zamierzonego przetwarzania. Organ nadzorczy informuje ADO, a gdy ma to zastosowanie także podmiot przetwarzający, o takim przedłużeniu w terminie miesiąca od wpłynięcia wniosku o konsultacje, z podaniem przyczyn tego opóźnienia. Bieg tych terminów można zawiesić, do czasu aż organ nadzorczy uzyska wszelkie informacje, których zażądał do celów konsultacji.
- 3) Konsultując się z organem nadzorczym zgodnie z ust. 1, ADO przedstawia mu:
  - a) gdy ma to zastosowanie – odpowiednie obowiązki administratora, współadministratorów oraz podmiotów przetwarzających uczestniczących w przetwarzaniu, w szczególności w przypadku przetwarzania w ramach grupy przedsiębiorstw;
  - b) cele i sposoby zamierzonego przetwarzania;
  - c) środki i zabezpieczenia mające chronić prawa i wolności osób, których dane dotyczą, zgodnie z niniejszym rozporządzeniem;
  - d) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych;

 Szpital Specjalistyczny w Prabutach sp. z o.o.	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
		Strona 60 z 81	
 Podmiot Lecznicy Samorządu Województwa Pomorskiego	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

- e) ocenę skutków dla ochrony danych, o której mowa w art. 35 Rozporządzenia PE; oraz
- f) wszelkie inne informacje, których żąda organ nadzorczy.

## **7. Zarządzanie ryzykiem w systemie ochrony danych osobowych**

- 1) Zarządzanie ryzykiem w systemie ochrony danych osobowych odbywa się we wszystkich komórkach organizacyjnych Szpitala Specjalistycznego w Prabutach Sp. z o.o. na podstawie Zał. nr 2 do POD.
- 2) Każdy kierownik komórki organizacyjnej, wyznaczony pracownik, mający wpływ na cele przetwarzania, jest odpowiedzialny za wykonanie co najmniej raz w roku identyfikacji ryzyka, szacowania ryzyka oraz wskazania działań zmierzających do redukcji ryzyka nieakceptowalnego w swoim zakresie odpowiedzialności.
- 3) Proces zarządzania ryzykiem dokumentowany jest na Arkuszu ryzyka w ochronie danych osobowych - z Form.4/POD.
- 4) Wypełnione Arkusze przedstawiane są do ADO/IOD do dnia 15 grudnia każdego roku.
- 5) Arkusze podlegają analizie oraz akceptacji ADO do dnia 15 stycznia każdego roku.
- 6) Po zatwierdzeniu przez ADO Arkuszy ryzyk wykonywany jest zbiorczy Arkusz ryzyk w ochronie danych osobowych dla Szpitala Specjalistycznego w Prabutach Sp. z o.o., który udostępnia się wszystkim pracownikom.
- 7) W przypadku wystąpienia incydentu lub naruszenia bezpieczeństwa w systemie ochrony danych osobowych w komórce organizacyjnej dokonywane jest ponowne szacowanie ryzyka – zgodnie z ustaleniami Zespołu ds. bezpieczeństwa.


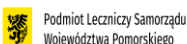
## **8. Powierzenie danych osobowych [28]**

Powierzenie danych osobowych realizowane jest w przypadku przekazywania danych osobowych zidentyfikowanych w Szpitalu Specjalistycznym w Prabutach Sp. z o.o., dla których Szpital jest Administratorem Danych, podmiotom zewnętrznym, które w rozumieniu Rozporządzenia, są Podmiotem przetwarzającym (nie stają się dla tych danych Administratorem).

Z każdym takim podmiotem zewnętrznym podpisywana jest umowa wg wzoru opracowanego na Form.9/POD – Umowa powierzenia danych osobowych.

Dopuszcza się również podpisanie dokumentu umowy powierzenia według innego wzoru, spełniającego jednak wszystkie kryteria zawarte w art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 r.

Utrzymywany jest Rejestr umów powierzenia danych osobowych - Form.8/POD.

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	PROCEDURA	Wydanie: 3	10.08.2025
		Strona 61 z 81	
	POLITYKA OCHRONY DANYCH OSOBOWYCH	Nr dokumentu: <b>7- Pr5</b>	

## 9. Obszar przetwarzania danych osobowych

Obszarem, w którym przetwarzane są dane osobowe są pomieszczenia znajdujące się w budynkach Szpitala Specjalistycznego w Prabutach Sp. z o.o., zlokalizowanych przy ulicy Kuracyjnej 30.

Budynki zabezpieczone systemem alarmowym, czujki ruchu zlokalizowane w kluczowych dla organizacji pomieszczeniach.

Szczególnym obszarem, w którym przetwarzane są dane osobowe i przebywać w nim mogą jedynie osoby zatrudnione z upoważnieniem do przetwarzania danych osobowych są pomieszczenie serwerowni, zlokalizowane w części administracyjnej Szpitala na poziomie 2. Dostęp do pomieszczenia, zabezpieczony zamkiem, klucz zdeponowany jest w Sekretariacie Szpitala. Przebywać w tym obszarze może tylko informatyk ,IOD oraz Zarząd Spółki. W każdym budynku Szpitala znajdują się Lokalne punkty dystrybucyjne, zabezpieczone również zamkami (szafy teledajcyjne), klucze zabezpieczone w pomieszczeniu serwerowni.

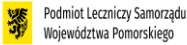
ADO utrzymuje Ewidencję osób upoważnionych do przetwarzania danych osobowych (Form.2/POD) na podstawie wystawionych, imiennych upoważnień do przetwarzania danych osobowych (Form.1/POD).

## 10. Rejestrowanie czynności przetwarzania [30]

Obowiązek prowadzenia rejestru czynności spoczywa na administratorze, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Obowiązek prowadzenia rejestrów kategorii czynności został nałożony zaś na podmioty przetwarzające, czyli osoby fizyczne lub prawne, organy publiczne, jednostki lub inne podmioty, które przetwarzają dane osobowe w imieniu administratora.

Tworząc system zarządzania bezpieczeństwem przetwarzania danych osobowych, należy przeprowadzić inwentaryzację wszystkich aktywów, jakimi dysponuje jednostka, rozumianych jako: informacje i związane z nimi procesy, systemy i sieci teleinformatyczne. Dla bezpieczeństwa danych osobowych – w tym dla zapewnienia, że dane osobowe udostępniane będą wyłącznie osobom do tego uprawnionym – inwentaryzacja taka powinna uwzględniać przyjęte zasady klasyfikacji przetwarzanych informacji. Przepisem Rozporządzenia PE zobowiązującym administratorów danych i podmioty przetwarzające do wprowadzenia takiej inwentaryzacji jest art. 30 dotyczący rejestrowania czynności przetwarzania.

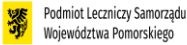
Rejestr czynności przetwarzania należy rozumieć jako wykaz przetwarzanych zbiorów danych („zbiór danych” oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie), na które dzieli się wszystkie przetwarzane u danego administratora danych informacje ze względu na: zakres przetwarzanych danych, cele przetwarzania oraz kategorie odbiorców, którym dane zostają udostępnione. Z wykazu tego jasno wynika, że przez pojęcie „czynności przetwarzania” nie należy rozumieć poszczególnych etapów przetwarzania danych w ramach danego zbioru –

<p>Szpital Specjalistyczny w Prabutach sp. z o.o.</p>  <p>Podmiot Leczniczy Samorządu Województwa Pomorskiego</p>	<p>PROCEDURA</p>	Wydanie: 3	10.08.2025
		Strona 62 z 81	
	<p>POLITYKA OCHRONY DANYCH OSOBOWYCH</p>	Nr dokumentu: <b>7- Pr5</b>	

takich jak pozyskiwanie danych, wysyłanie do podmiotów danych określonego rodzaju informacji, usuwanie danych oraz wykonywanie na zgromadzonych danych określonego rodzaju operacji (jak np. wykonywanie obowiązków IOD, lecz wszystkie operacje globalnie na określonym zbiorze danych. Granice takiego zbioru mają być wyznaczone nie przez poszczególne cząstkowe operacje przetwarzania, lecz przez wskaźniki wymienione odpowiednio w art. 30 ust. 1 pkt. a–g i w art. 30 ust. 2 pkt. a–d Rozporządzenia PE (takie jak: zakres danych, cel przetwarzania, kategorie ich odbiorców itp.), które pozwalają pogrupować wszystkie przetwarzane przez danego administratora dane w jeden lub kilka zbiorów.



1) Szpital Specjalistyczny w Prabutach Sp. z o.o. jako administrator danych osobowych prowadzi Rejestr czynności przetwarzania (Form.3A/POD), gdzie:

- IOD prowadzi rejestr wszystkich czynności przetwarzania, które wykonywane są w jego organizacji,
- czynności przetwarzania to zespół powiązanych ze sobą operacji na danych, wykonywanych przez jedną lub kilka osób, które można określić w sposób zbiorczy, w związku z celem, w jakim te czynności są podejmowane,
- przy wyodrębnianiu poszczególnych procesów (zespołów czynności) uwzględnia się rzeczywisty podział zadań pomiędzy poszczególnymi komórkami organizacyjnymi lub osobami w jednostce,
- Rejestr powinien obejmować opis poszczególnych zespołów operacji związanych zbiorczo z realizacją określonego celu przetwarzania, nie ma obowiązku opisywania każdej poszczególniej operacji wykonywanej na danych, takiej jak np. zbieranie, utrwalanie, porządkowanie, modyfikowanie, usuwanie (czy innej wskazanej w art. 4 pkt 2 Rozporządzenia PE),
- za odbiorcę uznaje się osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, z wyjątkiem organów publicznych, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego,
- podmiotami objętymi definicją odbiorcy będą podmioty przetwarzające, natomiast nie będą nimi inne podmioty działające z upoważnienia administratora, w jego imieniu i na jego polecenie wewnątrz struktury organizacyjnej,
- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 Rozporządzenia PE może mieć charakter ogólny i wskazywać najważniejsze założenia czy elementy przyjętych systemów lub koncepcji w zakresie bezpieczeństwa danych osobowych (jest to uzasadnione zwłaszcza w przypadkach, gdy koncepcje te obejmują wiele elementów i rozwiązań, które uszczegółowione są w innym miejscu, np. konkretnej dokumentacji, polityce lub procedurach; wówczas należy zamieścić w rejestrze ogólną informację o rodzaju zastosowanych zabezpieczeń (np. kontrola dostępu w oparciu o identyfikator i hasło, zastosowanie certyfikatów, szyfrowanie komunikacji itp.) oraz odesłanie do dokumentacji opisującej szczegóły zarządzania danego rodzaju zabezpieczeniami), jednak w każdym przypadku opis ten ma umożliwiać

<p>Szpital Specjalistyczny w Prabutach sp. z o.o.</p>  <p>Podmiot Leczniczy Samorządu Województwa Pomorskiego</p>	<p>PROCEDURA</p>	Wydanie: 3	10.08.2025
		Strona 63 z 81	
	<p>POLITYKA OCHRONY DANYCH OSOBOWYCH</p>	Nr dokumentu: <b>7- Pr5</b>	

administratorowi i podmiotowi przetwarzającemu oraz organowi nadzorczemu wstępną ocenę zastosowanych środków w odniesieniu do poszczególnych czynności i kategorii czynności zamieszczonych w rejestrze,

- w Rejestrze odnotowuje się fakt przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej wskazując nazwę tego państwa trzeciego lub organizacji międzynarodowej,
  - w Rejestrze dokumentuje się ocenę oraz odpowiednie zabezpieczenia, o których mowa w art. 49 ust. 1 akapit drugi Rozporządzenia PE,
  - gdy może być to przydatne w Rejestrze umieszcza się inne dane niż wymagane w art. 30 ust. 1 Rozporządzenia PE, w szczególności, gdy ułatwi to wykazanie zgodności z Rozporządzeniem PE w przypadku kontroli.
- 2) Szpital Specjalistyczny w Prabutach Sp. z o.o. prowadzi jako podmiot przetwarzający w imieniu innego administratora Rejestr kategorii czynności przetwarzania (Form.3B/POD), tylko w sytuacji gdy występuje jako Podmiot przetwarzający, gdzie:
- kategoria czynności przetwarzania (kategoria przetwarzania) to rodzaj usługi realizowanej przez podmiot przetwarzający na zlecenie administratora związanej ze zleconymi czynnościami przetwarzania,
  - rejestr czynności obejmuje wszystkie kategorie czynności przetwarzania dokonywane w imieniu wszystkich administratorów,
  - zawiera m.in. określenie (imię, nazwisko lub nazwę) każdego administratora, w imieniu którego działa podmiot przetwarzający oraz kategorie przetwarzania dokonywanych w imieniu każdego z administratorów,
  - w odniesieniu do każdego z administratorów wskazane jest zatem nazwanie poszczególnych powierzeń (zleceń), a zatem rodzaju usług, jakie podmiot przetwarzający na podstawie zawartych umów wykonuje na rzecz poszczególnych administratorów,
  - porządkuje się czynności wykonywane w ramach powierzenia w kategorii, czyli ich grupuje pod względem rodzaju usług świadczonych przez podmiot przetwarzający,
  - ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 Rozporządzenia PE może mieć charakter ogólny i wskazywać najważniejsze założenia czy elementy przyjętych systemów lub koncepcji w zakresie bezpieczeństwa danych osobowych (jest to uzasadnione zwłaszcza w przypadkach, gdy koncepcje te obejmują wiele elementów i rozwiązań, które uszczegółowione są w innym miejscu, np. konkretnej dokumentacji, polityce lub procedurach; wówczas należy zamieścić w rejestrze ogólną informację o rodzaju zastosowanych zabezpieczeń (np. kontrola dostępu w oparciu o identyfikator i hasło, zastosowanie certyfikatów, szyfrowanie komunikacji itp.) oraz odesłanie do dokumentacji opisującej szczegóły zarządzania danego rodzaju zabezpieczeniami) jednak w każdym przypadku opis ten ma umożliwiać administratorowi i podmiotowi przetwarzającemu oraz organowi nadzorczemu wstępną

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Lecznicy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
		Strona 64 z 81	
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

ocenę zastosowanych środków w odniesieniu do poszczególnych czynności i kategorii czynności zamieszczonych w rejestrze,

- w Rejestrze odnotowuje się fakt przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowe wskazując nazwę tego państwa trzeciego lub organizacji międzynarodowej,
- w Rejestrze dokumentuje się ocenę oraz odpowiednie zabezpieczenia, o których mowa w art. 49 ust. 1 akapit drugi Rozporządzenia PE.
- rejestr kategorii czynności może obejmować inne elementy niż wskazane w art. 30 ust. 2 Rozporządzenia PE, w szczególności takie, które podmiot przetwarzający uznaje za potrzebne i uzasadnione dla zapewnienia zgodności z prawem przetwarzania danych, które zostało mu powierzone.

W skład zbioru danych osobowych wchodzi: dokumentacja papierowa, urządzenia i oprogramowanie komputerowe służące do przetwarzania informacji oraz procedury przetwarzania danych w tym systemie oraz wydruki komputerowe.


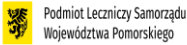
Wykaz zbiorów danych osobowych przetwarzanych w systemie informatycznym prowadzi ADO w formie pisemnej, w tym formie elektronicznej na Form.3A/POD – Rejestr czynności przetwarzania, a na Form.3B/POD – Rejestr kategorii czynności przetwarzania.

## **11. Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych [32]**

Do określenia środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych, wykorzystano wyniki przeprowadzonej oceny ryzyka dla obszaru ochrony danych osobowych. Takie podejście pozwoliło na wskazanie istniejących już zabezpieczeń i ocenę czy są one wystarczające dla zapewnienia ochrony danych osobowych. W obszarach ryzyka nieakceptowanego wdrażane są dodatkowe mechanizmy kontroli obszaru ochrony danych osobowych. Zasady oceny ryzyka zostały opisane w załączniku 1 do Polityki Ochrony Danych (Zał. 1/POD). W organizacji podczas szacowania ryzyk, nie stwierdzono ryzyka nieakceptowalnego, w związku z czym, nie wdrażano planów ciągłości działania.

### **11.1. Środki ochrony fizycznej**

- 1) Pomieszczenia w budynkach, w których nie przebywają pracownicy całą dobę, a, w których zlokalizowany jest obszar przetwarzania danych osobowych/informacji są zamykane po zakończeniu pracy. Budynek wyposażony w system alarmowy.
- 2) Urządzenia służące do przetwarzania danych osobowych/informacji zostają wyłączone po zakończeniu pracy, a pomieszczenia zamknięte.
- 3) Serwerownia umiejscowiona jest w zabezpieczonym poprzez zamknięte drzwi na klucz pomieszczeniu, dodatkowo dostęp do pomieszczenia zabezpieczony jest poprzez alarm, do

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Lecznicy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
		Strona 65 z 81	
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

przebywania w tym pomieszczeniu uprawnione są osoby tylko upoważnieniem w obecności *IOD, ASI lub Zarządu Szpitala.*



- 4) Przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych/informacji dopuszczane jest tylko w obecności osoby zatrudnionej przy przetwarzaniu danych lub w obecności ADO/IOD lub innej osoby upoważnionej.
- 5) Pomieszczenia tworzące obszar przetwarzania danych osobowych powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.
- 6) W przypadku przebywania osób postronnych w pomieszczeniach tworzących obszar przetwarzania danych osobowych powinny być ustawione w taki sposób, aby uniemożliwić im wgląd w dane.

## **11.2. Środki sprzętowe, informatyczne i telekomunikacyjne**

- 1) Każdy dokument papierowy przeznaczony do wyrzucenia powinien być uprzednio zniszczony w sposób uniemożliwiający jego odczytanie (w niszczarce).
- 2) System informatyczny oraz systemy przetwarzające dane zabezpieczone są przed nieupoważnionym dostępem osób trzecich z wykorzystaniem systemu autentykacji i autoryzacji użytkowników.
- 3) Serwery zabezpieczone na wypadek zaniku napięcia albo awarii w sieci zasilającej urządzeniami podtrzymującymi napięcie (UPS).
- 4) Na serwerach pracującym pod systemem Windows oraz wszystkich stacjach roboczych zainstalowano oprogramowanie antywirusowe. Poczta elektroniczna wpływająca do Szpitala Specjalistycznego w Prabutach Sp. z o.o. skanowana jest programem antywirusowym zarówno przed wysłaniem jak i podczas odbierania wiadomości.
- 5) Wdrożono system kopii zapasowych z wykorzystaniem nośników zewnętrznych.
- 6) Wykonane kopie zapasowe są okresowo testowane.
- 7) Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieupoważnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem i usuwa się niezwłocznie po ustaniu ich użyteczności, w sposób uniemożliwiający odczyt danych z nośnika.

## **11.3. Środki ochrony w ramach oprogramowania systemu**

- 1) Dostęp fizyczny do baz danych osobowych (tj. struktur baz danych) zastrzeżony jest wyłącznie dla ADO oraz osób przez niego wskazanych – ASI oraz firm współpracujących przy obsłudze informatycznej spółki, świadczących usługi nadzoru autorskiego do danych systemów, przy czym każde takie zdarzenie jest odnotowywane w odpowiednim rejestrze i poprzedzone kopią zapasową – Dziennik Administratora.
- 2) System informatyczny pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu.

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
		Strona 66 z 81	
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

#### **11.4. Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych**

- 1) Aplikacje służące do przetwarzania danych osobowych wymuszają stosowanie identyfikatora i hasła dostępu do danych na poziomie aplikacji, a tam gdzie jest to nie możliwe, w przypadku aplikacji jednostanowiskowych, na poziomie systemu operacyjnego.
- 2) Dla każdego użytkownika systemu ustalony jest odrębny identyfikator.
- 3) Zdefiniowano użytkowników i ich prawa dostępu do danych na poziomie aplikacji (unikalny identyfikator i hasło).

#### **11.5. Środki ochrony w ramach systemu użytkowego**



- 1) Zastosowano wygaszanie ekranu w przypadku dłuższej nieaktywności użytkownika, tj. powyżej 5 min.
- 2) Komputer, z którego możliwy jest dostęp do danych osobowych zabezpieczony jest hasłem uruchomieniowym spełniającym odpowiednie wymogi – minimum 8 znaków, mała, duża litera, znak specjalny lub cyfra.

#### **11.6. Środki organizacyjne**

- 1) Administrator Danych powołał Inspektora Ochrony Danych w Szpitalu Specjalistycznym w Prabutach Sp. z o. o.
- 2) Wydano dokumentację opisującą funkcjonowanie systemu ochrony danych osobowych w Szpitalu Specjalistycznym w Prabutach Sp. z o.o. – Politykę Ochrony Danych.
- 3) Osoby upoważnione do przetwarzania danych osobowych przed dopuszczeniem do pracy są zawsze szkolone w zakresie obowiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych i informacji funkcjonujących w Szpitalu Specjalistycznym w Prabutach Sp. z o.o. oraz poinformowane o podstawowych zagrożeniach związanych z przetwarzaniem danych w systemie informatycznym.
- 4) Prowadzona jest ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych (Form.2/POD – Rejestr osób upoważnionych do przetwarzania danych osobowych).
- 5) Wprowadzono identyfikację ryzyk w systemie ochrony danych osobowych oraz proces zarządzania ryzykiem.
- 6) Prowadzone są systematyczne szkolenia w zakresie wymagań prawnych oraz wymagań własnych związanych z systemem ochrony danych, w szczególności w przypadku zmian w przepisach zewnętrznych.
- 7) Zdefiniowano procedury postępowania w sytuacji naruszenia ochrony danych osobowych.
- 8) Wprowadzono obowiązek rejestracji wszystkich incydentów związanych z ochroną danych osobowych i naruszaniem bezpieczeństwa informacji.
- 9) Zawierane są umowy powierzenia danych osobowych z podmiotami zewnętrznymi.

#### **11.7. Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych**



Do zapoznania się z niniejszym dokumentem oraz stosowania zawartych w nim zasad zobowiązani są wszyscy pracownicy Szpitala Specjalistycznego w Prabutach Sp. z o.o.

 Szpital Specjalistyczny w Prabutach sp. z o.o.	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
		Strona 67 z 81	
 Podmiot Lecznicy Samorządu Województwa Pomorskiego	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

upoważnieni do przetwarzania danych. Niezastosowanie się do wprowadzonej przez Administratora Danych Polityki Ochrony Danych, której założenia określa niniejszy dokument, i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych będzie potraktowane jako naruszenie obowiązków pracowniczych.

## **ZASADY POSTĘPOWANIA DLA UŻYTKOWNIKÓW :**

- 1) Kasowanie po wykorzystaniu danych na dyskach przenośnych.
- 2) Zachowanie tajemnicy danych, w tym także wobec najbliższych.
- 3) Pilne strzeżenie akt, płyt CD/DVD, pamięci przenośnych i komputerów przenośnych.
- 4) Nie pozostawianie bez kontroli dokumentów, nośników danych.
- 5) Ustawianie ekranów komputerowych tak, aby osoby nie powołane nie mogły oglądać ich zawartości, a zwłaszcza nie naprzeciwko wejścia do pomieszczenia oraz nie skierowane ekranem do okna.
- 6) Nie zapisywanie hasła wymaganego do uwierzytelnienia się w systemie na papierze lub innym nośniku.
- 7) Nie podłączanie do listew podtrzymujących napięcie, przeznaczonych dla sprzętu komputerowego, innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejników, czajników, wentylatorów).
- 8) Dbanie o prawidłową wentylację komputerów.
- 9) Powstrzymanie się przez osoby upoważnione do przetwarzania danych osobowych od samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu.
- 10) Bezwzględnie zabronione jest samodzielne dokonywanie przez użytkowników napraw sprzętu informatycznego, wymiany jego podzespołów oraz wykonywania innych czynności nie związanych bezpośrednio z jego eksploatacją lub nie dopuszczonych do wykonywania przez producenta sprzętu w instrukcji obsługi.
- 11) Przestrzeganie przez osoby upoważnione do przetwarzania danych osobowych swoich uprawnień w systemie, tj. właściwego korzystania z aplikacji, używania tylko własnego identyfikatora i hasła.
- 12) Nie pozostawianie osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe/informacje, bez obecności osoby upoważnionej do przetwarzania danych osobowych.
- 13) Opuszczanie stanowiska pracy dopiero po aktywizowaniu wygaszacza ekranu (klawisze WIN+L) lub po zablokowaniu stacji roboczej w inny sposób.
- 14) Obowiązuje całkowity zakaz robienia kopii całych zbiorów danych oraz informacji, za wyjątkiem kopii wykonywanych w ramach cyklicznych backupów danych.
- 15) Udostępnianie danych osobowych pocztą elektroniczną tylko w postaci zaszyfrowanej.
- 16) Nie wnoszenie poza obszar Szpitala Specjalistycznego w Prabutach Sp. z o.o. na jakichkolwiek nośnikach zbiorów danych i danych osobowych i informacji bez zgody ADO.
- 17) Wykonywanie kopii roboczych danych, na których się właśnie pracuje, tak często, aby zapobiec ich utracie.

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
		Strona 68 z 81	
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

- 18) Kończenie pracy na stacji roboczej po wprowadzeniu danych przetwarzanych tego dnia w odpowiednie obszary serwera, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w UPS i listwie.
- 19) Niszczanie w niszczarce lub chowanie do szaf zamykanych na klucz wszelkich wydruków zawierających dane osobowe, przed opuszczeniem miejsca pracy i po zakończeniu dnia pracy.
- 20) Chowanie do zamykanych na klucz szaf wszelkich akt zawierających dane osobowe, przed opuszczeniem miejsca pracy i po zakończeniu dnia pracy.
- 21) Umieszczanie kluczy do szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy.
- 22) Zamykanie okien w razie opadów lub innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych.
- 23) Zamykanie okien w razie opuszczenia pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy.
- 24) Zamykanie drzwi na klucz po zakończeniu pracy w danym dniu.
- 25) Zabezpieczenia kluczy do drzwi wejściowych do pomieszczeń Szpitala Specjalistycznego w Prabutach Sp. z o.o., w taki sposób aby nie zostały utracone.
- 26) Wszelkie urządzenia mobilne mogą być wynoszone poza obszar przetwarzania danych i informacji (siedziba Szpitala Specjalistycznego w Prabutach Sp. z o.o.) wyłącznie za zgodą ADO. Dane te muszą być objęte ochroną kryptograficzną. Pracownik wynoszący urządzenie mobilne jest całkowicie odpowiedzialny za dane, informacje na nim zawarte oraz bezpieczeństwo samego nośnika.


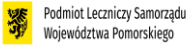
**UWAGA:**

**Nie zastosowanie się do powyższych zasad przez pracownika oraz osób zatrudnionych na umowach zlecenia czy innych umowach cywilnoprawnych w Szpitalu Specjalistycznym w Prabutach Sp. z o.o., które będzie skutkowało wystąpieniem incydentu bezpieczeństwa narażającym na starty finansowe i wizerunkowe Szpitala Specjalistycznego w Prabutach Sp. z o.o., spowoduje wystąpienie do pracownika oraz osób zatrudnionych na umowach zlecenia czy innych umowach cywilnoprawnych z roszczeniem o naprawienie szkody zgodnie z Kodeksem Pracy.**

## **12. Sprawdzanie systemu ochrony danych osobowych [39]**

ADO raz w roku, dokona podsumowania funkcjonowania systemu ochrony danych osobowych i bezpieczeństwa informacji w Szpitalu Specjalistycznym w Prabutach Sp. z o.o.. Zapisów z podsumowania dokona na Form.5/POD – Roczne sprawozdanie z funkcjonowania systemu ochrony danych osobowych i bezpieczeństwa informacji.

W tym celu realizowany jest audyt wewnętrzny systemu ochrony danych wykonywany przez Inspektora Ochrony Danych Osobowych lub osobę przez niego upoważnioną z wykorzystaniem ASI lub innej osoby przez wskazane przez ADO.

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
		Strona 69 z 81	
<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>		Nr dokumentu: <b>7- Pr5</b>	

1) Definicje:

- **Audyt wewnętrzny systemu ochrony danych osobowych** – należy przez to rozumieć czynności mające na celu zweryfikowanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz wymaganiami zawartymi w Polityce Ochrony Danych.
- **Audytór wewnętrzny** – osoba wykonująca audyt wewnętrzny.
- **Audytowany** – osoba, u której wykonywany jest audyt wewnętrzny.
- **Niezgodność** – niespełnienie wymagania zawartego w przepisie prawnym zewnętrznym, przepisach wewnętrznych, dokumentacji opisującej system ochrony danych osobowych w Szpital Specjalistyczny w Prabutach Sp. z o.o..
- **Sprawozdanie** – należy przez to rozumieć dokument, opracowany przez *wykonującego audyt*, zaakceptowany przez ADO wytworzony po dokonaniu audytu wewnętrznego systemu ochrony danych osobowych zawierający podsumowanie funkcjonowania systemu ochrony danych osobowych i jego ocenę.

2) Procedura postępowania

IOD przygotowuje **Plan audytów wewnętrznych** systemu ochrony danych osobowych w cyklu rocznym wskazując komórki organizacyjne, które podlegać będą audytowi. W Planie audytów określony jest przedmiot, zakres oraz termin przeprowadzenia poszczególnych sprawdzeń. W tym celu przygotowuje Form 6/POD. W cyklu rocznym audytem objęte są wszystkie komórki organizacyjne. ADO zatwierdza plan audytów w cyklu rocznym.

Zakres sprawdzenia obejmuje weryfikację wymagań zawartych:



- w Rozporządzeniu PE,
- w ustawie o ochronie danych osobowych,
- w dokumentacji systemu ochronnych danych osobowych,

w szczególności:

- 1) opracowanie i kompletności dokumentacji przetwarzania danych;
- 2) zgodność dokumentacji przetwarzania danych z obowiązującymi przepisami prawa;
- 3) stan faktyczny w zakresie przetwarzania danych osobowych;
- 4) zgodność ze stanem faktycznym przewidzianych w dokumentacji przetwarzania danych środków technicznych i organizacyjnych służących przeciwdziałaniu zagrożeniom dla ochrony danych osobowych;
- 5) przestrzeganie zasad i obowiązków określonych w dokumentacji przetwarzania danych.

**Audyt doraźny** jest przeprowadzany niezwłocznie po powzięciu wiadomości przez ADO/IOD o naruszeniu ochrony danych osobowych lub incydencie bezpieczeństwa albo o uzasadnionym podejrzeniu takiego naruszenia.

IOD lub osoba przeprowadzająca audyt wewnętrzny przygotowuje **Listę pytań kontrolnych/check-listę** (Form.7/POD), która obejmuje zakresem wymagania Rozporządzenia PE, ustawy o ochronie danych osobowych oraz wymagania własne organizacji zawarte w Polityce Ochrony Danych. Na dokumencie Listy odnotowywane są obiektywne dowody

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
		Strona 70 z 81	
<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>		Nr dokumentu: <b>7- Pr5</b>	

(dokumenty, zapisy, w tym tworzone w systemach elektronicznych, oświadczenia, obserwacje) potwierdzające (lub nie) spełnienie wymagań zawartych we wskazanych wyżej dokumentach. Do każdego pytania na odwrocie odnotowuje się obiektywny dowód.

W przypadku wykrycia podczas weryfikacji niezgodności Audytor ustala wspólnie z audytowanym ich przyczyny i po uzgodnieniu z ADO zaleca wdrożenie działań korekcyjnych (usuwających niezgodności) i korygujących (usuwających przyczyny zaistniałych niezgodności). Ustalenia zapisywane są w sprawozdaniu. Podczas kolejnego sprawdzenia sprawdzana jest skuteczność wykonanych działań.

Pracownik odpowiedzialny za obszar danych osobowych, którego dotyczy sprawdzenie (dotyczy to również ASI) jest zobowiązany udostępnić wszystkie żądane dane, dokumenty, zapisy, udzielić wyczerpujących wyjaśnień oraz dokonywać okazania pomieszczeń, urządzeń na życzenie sprawdzającego oraz zapewnić pełną, merytoryczną współpracę.

Po zakończeniu sprawdzenia ADO/IOD przygotowuje **Sprawozdanie** na Form.5/POD – Sprawozdanie z funkcjonowania systemu ochrony danych osobowych.

### **13. Procedura postępowania w przypadku naruszenia bezpieczeństwa systemu ochrony danych osobowych [33]**

Osoby zatrudnione przy przetwarzaniu danych osobowych w Szpital Specjalistyczny w Prabutach Sp. z o.o. są zobowiązane powiadomić ADO/IOD o ewentualnych naruszeniach bezpieczeństwa systemu ochrony danych osobowych w każdym zbiorze danych lub systemie celem podjęcia dalszych działań, dążących do minimalizacji skutków wystąpienia tego incydentu.


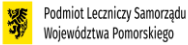
**Incydent bezpieczeństwa (naruszenie ochrony danych osobowych)** to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem:

- zniszczenia,
- utracenia,
- zmodyfikowania,
- nieuprawnionego ujawnienia,
- nieuprawnionego dostępu do danych osobowych, przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Każdy incydent / zdarzenie potencjalnie naruszające bezpieczeństwo danych osobowych podlega raportowaniu na Form.11/POD – Raport z incydentu / zdarzenie potencjalnie naruszającego bezpieczeństwo danych/informacji. Do Raportu zostaną dołączone dowody z postępowania, w tym dowody z naruszenia wdrożonych zabezpieczeń.

Utrzymywany jest Form.10/POD – Rejestr incydentów / zdarzeń potencjalnie naruszających bezpieczeństwo informacji.



1) Osoba, która zauważy incydent bezpieczeństwa zawiadamia o tym fakcie ADO/IOD niezwłocznie po ujawnieniu zdarzenia.

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	PROCEDURA	Wydanie: 3	10.08.2025
		Strona 71 z 81	
	POLITYKA OCHRONY DANYCH OSOBOWYCH	Nr dokumentu: <b>7- Pr5</b>	

- 2) ADO wskazuje osobę, która zbiera dowody dotyczące naruszenia ochrony danych osobowych/incydentu bezpieczeństwa oraz wypełnia Raport z incydentu. Wypełniony Raport z incydentu przekazany jest do ADO w terminie 24 godzin od odnotowania naruszenia/incydentu.
- 3) Po otrzymaniu Raportu z incydentu ADO zwołuje Zespół ds. bezpieczeństwa informacji, w którego skład wchodzi: ADO, IOD, ASI, kierownik komórki organizacyjnej, w której nastąpiło naruszenie celem podjęcia decyzji związanych z zawiadomieniem organu nadzorczego oraz ewentualnego zawiadomienia osób, jeżeli naruszenie ochrony danych osobowych zawiera ryzyko lub wysokie ryzyko naruszenia prawa do wolności osób fizycznych. Z obrad Zespołu sporządzana jest notatka służbowa.
- 4) Zespół ds. bezpieczeństwa danych osobowych dokonuje przeglądu stosowanych zabezpieczeń organizacyjnych i technicznych w kontekście ujawnionego incydentu, w szczególności dokonuje przeglądu procesu zarządzania ryzykiem w tym obszarze. Zespół bezpieczeństwa danych osobowych dokonuje ponownego szacowania ryzyka w celu stwierdzenia czy incydent stanowi ryzyko naruszenia praw i wolności osób, których dane dotyczą lub wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą.

**UWAGA: ryzyko naruszenia praw i wolności osób fizycznych** może prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych głównie w następujących przypadkach:

1. jeżeli przetwarzanie może skutkować dyskryminacją, kradzieżą tożsamości, oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną;
  2. jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi;
  3. jeżeli przetwarzane są dane osobowe (**wrażliwe**) ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i czynów zabronionych lub związanych z tym środków bezpieczeństwa;
  4. jeżeli oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych (**profilowanie**);
  5. jeżeli przetwarzanie dotyczy **dużej ilości danych osobowych** i wpływa na dużą liczbę osób, których dane dotyczą.
- 5) Pozostałe wytyczne postępowania w przypadku Naruszenia ochrony danych osobowych [33 i 34] zostały opisane w punkcie 4 POD.

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
		Strona 72 z 81	
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

## **14. Zarządzanie systemami informatycznymi, w których przetwarzane są dane osobowe**


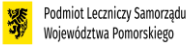
Zasady i tryb postępowania z systemami informatycznymi, w których przetwarzane są dane osobowe, tj.:

- procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności (14.1),
- stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem (14.2),
- procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu (14.3),
- procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania i ich przechowywanie (14.4),
- sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe (14.5),
- sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania złośliwego (14.6),
- procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych (14.7).

Powyższe zasady określone mają zastosowanie do wszystkich osób upoważnionych przez ADO do przetwarzania danych osobowych w zakresie zgodnym z zakresem ich obowiązków i uprawnień.

### **14.1. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności**

- 1) Dostęp do sieci informatycznej, systemów informatycznych i programów zabezpieczony jest systemem użytkowników i haseł oraz ograniczaniem dostępu do zasobów sieci. Identyfikator i hasło jednoznacznie identyfikują, weryfikują i autoryzują tożsamość użytkownika.
- 2) Rejestracji użytkowników w systemie dokonuje ASI.
- 3) W systemie informatycznym rejestrowani mogą być wyłącznie użytkownicy, którym ADO wydał upoważnienia do przetwarzania danych osobowych.
- 4) Uprawnienia na poziomie Administratora Systemu Informatycznego posiada ADO, uprawnienia te może realizować również osoba upoważniona przez ADO, pod jego nadzorem.
- 5) Użytkownikom nadawane są uprawnienia do pracy tylko w wymaganych dla realizacji powierzonych zadań modułach i funkcjach programów. Wszelkie zmiany w tym zakresie potwierdzane są na Form.2/POD – Rejestr osób upoważnionych do przetwarzania danych osobowych.
- 6) Wyłączenie użytkownika z ewidencji osób upoważnionych do przetwarzania danych osobowych obliguje ASI do odebrania temu użytkownikowi dostępu do danych osobowych przetwarzanych w systemie informatycznym oraz do zablokowania dostępu do wszystkich

 Szpital Specjalistyczny w Prabutach sp. z o.o.	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
		Strona 73 z 81	
 Podmiot Lecznicy Samorządu Województwa Pomorskiego	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	


systemów informatycznych, do których miał uprawnienia. Natomiast identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych nie jest usuwany z systemu informatycznego i nie jest przydzielany innej osobie.

## **14.2. Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem**

- 1) Użytkownik jest w pełnym zakresie odpowiedzialny za swoje hasło, w tym za jego okresowe zmienianie i utrzymywanie w tajemnicy.
- 2) Użytkownik jest w pełnym zakresie odpowiedzialny za dostosowanie hasła do opisanych niżej obowiązujących reguł, jeśli przestrzegania tych reguł nie wymusza w sposób automatyczny system informatyczny lub oprogramowanie.
- 3) Żaden z użytkowników, nie może mieć możliwości uzyskania z systemu informatycznego aktualnego lub nieważnego hasła innego użytkownika.
- 4) ADO/ASI musi mieć możliwość zmiany hasła użytkownika bez znajomości aktualnego lub nieważnego hasła użytkownika.
- 5) Hasło użytkownika nie może być takie samo jak identyfikator użytkownika.
- 6) Hasło użytkownika musi składać się z co najmniej 8 znaków, wskazane jest, by zawierało małą i dużą literę, cyfrę lub znak specjalny.
- 7) Hasło użytkownika musi być zmieniane nie rzadziej niż co 30 dni. Hasło użytkownika musi być zmienione niezwłocznie w przypadku jego ujawnienia lub podejrzenia ujawnienia.
- 8) Użytkownik jest zobowiązany do utrzymania swoich haseł w tajemnicy, również po utracie ich ważności.
- 9) Hasło przy wpisywaniu nie może być w sposób jawny wyświetlane na ekranie.
- 10) Hasło nie może być automatycznie zapisane w programie.
- 11) Hasła administracyjne pozostają również w dyspozycji ADO. Przechowuje się je w zabezpieczonym miejscu. Otwarcie koperty, w którym są przechowywane, może nastąpić wyłącznie w przypadku uzasadnionej konieczności na polecenie z Administratora Danych.

## **14.3. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu**

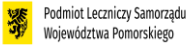
- 1) ASI monitoruje rozpoczęcie i zakończenie pracy systemu informatycznego.
- 2) ASI ma prawo do monitorowania pracy urządzeń przyłączonych do sieci informatycznej pod kątem przesyłania i przetwarzania danych, rejestracji zdarzeń związanych z przesyłaniem i przetwarzaniem danych w oprogramowaniu oraz prawidłowości wykorzystania powierzonego użytkownikom sprzętu i oprogramowania.
- 3) Przed rozpoczęciem pracy na komputerze użytkownik musi dokonać autoryzacji podczas logowania do systemu operacyjnego, dopiero po pomyślnej autoryzacji użytkownik może uruchomić aplikację służącą do przetwarzania danych osobowych, dokonując osobnej autoryzacji podczas uruchamiania tej aplikacji.
- 4) Kontrola przetwarzanych danych prowadzona jest na bieżąco przez użytkownika na każdym stanowisku merytorycznym. Nadzór prowadzi bezpośredni przełożony użytkownika, i w trybie audytów wewnętrznych wykonywanych przez IOD lub osobę przez niego upoważnioną.

<p>Szpital Specjalistyczny w Prabutach sp. z o.o.</p>  <p>Podmiot Leczniczy Samorządu Województwa Pomorskiego</p>	<p><b>PROCEDURA</b></p>	<p>Wydanie: 3</p>	<p><b>10.08.2025</b></p>
		<p>Strona 74 z 81</p>	
	<p><b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b></p>	<p>Nr dokumentu: <b>7- Pr5</b></p>	

- 5) W przypadku konieczności czasowego opuszczenia stanowiska pracy przyłączonego do sieci informatycznej lub służącego przetwarzaniu danych wiążącego się ze stratą z pola widzenia swojego stanowiska, użytkownik powinien: wylogować się z programu lub sieci informatycznej lub zablokować stację roboczą odpowiednią kombinacją klawiszy (WIN+L), przy czym odblokowanie może nastąpić dopiero po podaniu hasła, lub dopilnować konfiguracji wygaszacza ekranu w ten sposób, aby powrót do normalnej pracy był możliwy dopiero po podaniu hasła.
- 6) Każdy użytkownik jest zobowiązany do zadbania, aby niemożliwe było odczytanie informacji z monitora przez osoby nieuprawnione.
- 7) Użytkownik jest zobowiązany do wyrejestrowania się z systemu informatycznego przed wyłączeniem stacji roboczej.
- 8) W sytuacji naruszenia lub podejrzenia naruszenia bezpieczeństwa systemu, użytkownicy zobowiązani są do bezzwłocznego powiadomienia o tym fakcie Administratora Danych Osobowych i/lub Inspektora Ochrony Danych.

#### **14.4. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania**

- 1) Kopią zapasową objęte są dane znajdujące się przede wszystkim na serwerach. Za wykonywanie kopii zapasowych zlokalizowanych na serwerze odpowiedzialny jest ASI. Z takiej czynności powinien zostać zapis (forma elektroniczna lub papierowa). Natomiast w przypadku stanowisk w których uniemożliwione jest wykonanie kopii zapasowych przez ASI, za wykonywanie kopii zapasowych odpowiedzialni są użytkownicy lokalnie na swoich stanowiskach.
- 2) Kopia zapasowa danych gromadzonych na serwerze wykonywana jest przez kopiowanie całości danych. Harmonogram sporządzania kopii zapasowych musi gwarantować dostępność w każdej chwili dwóch kopii: z końca każdego kwartału oraz z końca ubiegłego roku. Kopie codzienne zapisywane są na lokalnym dysku twardym komputera znajdującego się pod stałym nadzorem ASI. Kopie kwartalne i roczne zapisywane są na nośnikach optycznych, które przechowywane są w zamkniętej szafie. Kopie codzienne są usuwane po zapisaniu kopii tygodniowej na nośnik optyczny.
  - a) Kopie awaryjne tworzone są przed każdą aktualizacją systemu informatycznego, składników systemu informatycznego lub poszczególnych programów służących do przesyłania lub przetwarzania danych. Kopie awaryjne zapisywane są na lokalnym dysku twardym komputera znajdującego się pod stałym nadzorem ASI.
  - b) Po wykonaniu kopii zapasowej i awaryjnej ASI ma obowiązek sprawdzić poprawność i kompletność skopiowanych danych. Z testu odtworzeniowego należy sporządzić **zapis**.
  - c) Kopie zapasowe na nośnikach optycznych przechowywane są w zamkniętym sejfie, do której dostęp ma wyłącznie ADO/IOD, ASI.
  - d) Kopie zapasowe usuwa się niezwłocznie w wypadku ich uszkodzenia lub po utracie terminu przechowywania, w sposób trwale uniemożliwiający ich odczytanie.
  - e) Kopie zapasowe przechowywane są przez okres:
    - kwartalne – co najmniej do końca roku kalendarzowego, dopuszcza się dłuższy okres przechowywania, o ile pozwalają na to warunki,
    - roczne - nieograniczone.



Szpital Specjalistyczny w Prabutach sp. z o.o.   Podmiot Leczniczy Samorządu Województwa Pomorskiego	PROCEDURA	Wydanie: 3	10.08.2025
		Strona 75 z 81	
	POLITYKA OCHRONY DANYCH OSOBOWYCH	Nr dokumentu: <b>7- Pr5</b>	

#### 14.5. Sposób, miejsce i okres przechowywania papierowych i elektronicznych nośników informacji zawierających dane osobowe

- 1) Wydruki archiwalne lub bieżące przechowywane mogą być wyłącznie w pomieszczeniach uniemożliwiających dostęp do nich przez osoby nieupoważnione.
- 2) Za bezpieczeństwo danych zapisanych w komputerach przenośnych oraz w innych urządzeniach przenośnych w całości odpowiada użytkownik komputera lub urządzenia przenośnego, przy czym dane osobowe są przetwarzane jedynie w sieci lokalnej przewodowej z wykorzystaniem terminali stacjonarnych i bez zgody ADO nie można ich zapisywać na komputerach bądź urządzeniach przenośnych.
- 3) Zbędne wydruki zawierające dane osobowe natychmiast po wykorzystaniu muszą zostać zniszczone w niszczarce dokumentów.
- 4) Przeznaczone do likwidacji elektroniczne i optyczne nośniki informacji, mogące zawierać dane osobowe, pozbawia się w sposób trwały zapisu tych danych, a w przypadku gdy nie jest to możliwe, niszczy lub uszkadza się w sposób trwale uniemożliwiający ich odczytanie. Za niszczenie zbędnych nośników elektronicznych odpowiada ASI. Z likwidacji sporządza się **zapis**.
- 5) Za zniszczenie zbędnych wydruków i innych zbędnych dokumentów zawierających dane osobowe odpowiedzialny jest każdy pracownik na swoim stanowisku pracy, chyba że dokumenty te trafiły w sposób przypadkowy do użytkownika. W takim przypadku należy dokumenty te niezwłocznie przekazać do ADO/IOD.
- 6) W przypadku konieczności przekazywania elektronicznych lub optycznych nośników informacji zawierających dane osobowe podmiotom zewnętrznym w sytuacjach nie związanych z wykonywanymi działaniami służbowymi, nośniki te pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie. W przypadku napraw sprzętu – przeprowadzane są one na miejscu w siedzibie pod nadzorem ASI.
- 7) Wszelkie nośniki zewnętrzne na których przechowywane są kopie zapasowe przechowywane są w zamkniętym na klucz sejfie który znajduje się w pomieszczeniu serwerowni.

#### 14.6. Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania złośliwego



- 1) Za aktualność stosowanych zabezpieczeń, dostosowywanie do aktualnych potrzeb, konfigurację i zarządzanie nimi odpowiada ASI.
- 2) W przypadku zauważonych niedociągnięć w zakresie zapewnienia bezpieczeństwa systemu informatycznego należy je zgłaszać na piśmie (e-mail) ADO/IOD.
- 3) Wykorzystywane rozwiązania muszą zapewnić automatyczne działania w przypadku wykrycia zagrożenia w systemie informatycznym oraz zapewnić możliwość konfiguracji odpowiednio do potrzeb. Minimalnym automatycznym działaniem jest zablokowanie możliwości pracy w systemie do chwili podjęcia decyzji o sposobie postępowania w przypadku wykrycia zagrożenia.
- 4) W przypadku, gdy system zabezpieczeń wskazuje zaistnienie zagrożenia, użytkownicy są zobowiązani bezzwłocznie powiadomić o tym fakcie ASI, który po jego usunięciu sprawdza system i przywraca go do pełnej funkcjonalności. ASI niezwłocznie zawiadamia o tym fakcie oraz podjętych działania ADO/IOD (na piśmie – e-mail).

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
			Strona 76 z 81
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

- 5) Bezwzględnie zakazuje się użytkownikom samowolnego korzystania z prywatnych lub pochodzących ze źródła innego niż miejsce pracy nośników informacji (magnetycznych, optycznych, urządzeń podłączanych do stacji roboczych). Korzystanie z takich nośników może mieć miejsce wyłącznie po uzyskaniu zgody ADO/IOD, po uprzednim sprawdzeniu nośnika informacji przez ASI pod względem bezpieczeństwa dla systemu informatycznego.
- 6) Bezwzględnie zakazuje się użytkownikom samowolnego instalowania na stacjach roboczych jakiegokolwiek oprogramowania z jakiegokolwiek źródła, za wyjątkiem aktualizowanych automatycznie komponentów systemu operacyjnego.
- 7) W przypadku konieczności zainstalowania innego oprogramowania niż to, które otrzymuje do dyspozycji na powierzonej mu stacji roboczej, użytkownik zgłasza taką potrzebę ADO/IOD wraz z uzasadnieniem. ASI w porozumieniu z ADO/IOD (w przypadkach wymagających konsultacji) decyduje o rzeczywistym zaistnieniu takiej konieczności. W przypadku pozytywnej opinii jedyną osobą uprawnioną do zainstalowania dodatkowego oprogramowania jest ASI.
- 8) Bezwzględnie zabrania się użytkownikom łamania lub obchodzenia zabezpieczeń systemów informatycznych. O każdym przypadku znalezienia luki w zabezpieczeniach użytkownik ma obowiązek powiadomić ADO/IOD.
- 9) Użytkownicy są bezpośrednio odpowiedzialni za zainstalowane na powierzonych im stacjach roboczych oprogramowanie oraz mają obowiązek zgłaszać wszelkie wątpliwości w tym zakresie ADO/IOD i/lub ASI, ze szczególnym uwzględnieniem zmian, które zostały wprowadzone podczas ich nieobecności.
- 10) Wszystkie stacje robocze są chronione przez oprogramowanie antywirusowe aktualizowane automatycznie codzienne.

#### **14.7. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych**

- 1) Przeglądu i konserwacji sprzętu w sieci informatycznej, systemów informatycznych i nośników informacji dokonuje bądź nadzoruje stosownie do potrzeb ASI. Fakt dokonania odnotowuje w Dzienniku Administratora – Form.12/IPOD.
- 2) Przegląd wszystkich aktywów odbywa się co najmniej raz w roku.
- 3) W przypadku przekazywania stacji roboczej z dyskiem albo innych nośników informacji do naprawy na zewnątrz organizacji, dysk lub nośnik jest demontowany, pozbawiany wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie lub naprawa dokonywana jest w obecności ASI. Fakt zniszczenia nośnika informacji, na którym były gromadzone dane osobowe odnotowuje się na Form.13/POD - Protokół zniszczenia uszkodzonych nośników.
- 4) W przypadku awarii systemu informatycznego i utraty informacji lub w przypadku zaistnienia możliwości uszkodzenia informacji ASI jest zobowiązany do:
  - przetestowania sieci informatycznej, systemu informatycznego oraz aplikacji służącej do przetwarzania danych,
  - oceny zasadności odtworzenia danych przy wykorzystaniu aktualnej kopii zapasowej lub kilku kopii zapasowych,
  - w przypadku uzasadnionej konieczności odtworzyć dane przy wykorzystaniu aktualnej kopii zapasowej lub kilku kopii zapasowych.

 Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
			Strona 77 z 81
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

## 15. Postanowienia końcowe

- 1) Nieprzestrzeganie zasad postępowania określonych w Polityce Ochrony Danych stanowi naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności dyscyplinarnej określonej w Kodeksie Pracy.
- 2) Jeżeli skutkiem działań jest ujawnienie informacji osobie nieupoważnionej, sprawca może zostać pociągnięty do odpowiedzialności karnej wynikającej z przepisów Kodeksu Karnego oraz ustawy o ochronie danych osobowych.
- 3) Jeżeli skutkiem działań jest szkoda, sprawca ponosi odpowiedzialność materialną na warunkach określonych w przepisach Kodeksu Pracy oraz Prawa Cywilnego.


Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest przed dopuszczeniem do przetwarzania danych zapoznać się z:

- niniejszym dokumentem,
- wymaganiami Rozporządzenia PE, Ustawy i aktami wykonawczymi dotyczącymi ochrony danych osobowych,
- zarządzeniami w sprawie wprowadzenia dokumentacji przetwarzania danych osobowych w Szpitalu Specjalistycznym w Prabutach Sp. z o.o.

oraz złożyć stosowne oświadczenie, potwierdzające znajomość treści tych dokumentów.

## 16. Załączniki

- Form.1/POD – Upoważnienie do przetwarzania danych osobowych
- Form.2/POD – Rejestr osób upoważnionych do przetwarzania danych osobowych
- Form.3A/POD – Rejestr czynności przetwarzania
- Form.3B/POD – Rejestr kategorii czynności przetwarzania
- Form.4/POD – Arkusz ryzyka w ochronie danych osobowych
- Form.5/POD – Roczne sprawozdanie z funkcjonowania systemu ochrony danych osobowych i bezpieczeństwa informacji
- Form.6/POD – Plan audytów wewnętrznych systemu ochrony danych osobowych
- Form.7/POD – Lista kontrolna – IOD/ADO
- Form.8/POD – Rejestr umów powierzenia
- Form.9/POD – Umowa powierzenia danych osobowych
- Form.10/POD – Rejestr incydentów związanych z ochroną danych osobowych
- Form.11/POD - Raport z incydentu / zdarzenia potencjalnie naruszającego bezpieczeństwo danych
- Form.12/POD – Dziennik Administratora
- Form.13/POD – Protokół zniszczenia uszkodzonych nośników
- Zał. 1/POD – Metodologia oceny ryzyka w ochronie danych osobowych
- Zał. 2/POD – Wykaz aktów prawnych w zakresie przetwarzania danych osobowych
- Zał. 3/POD – Polityka czystego biura i czystego pulpitu
- Zał. 4/POD – Zgłoszenie incydentu
-

Szpital Specjalistyczny w Prabutach sp. z o.o.  Podmiot Leczniczy Samorządu Województwa Pomorskiego	<b>PROCEDURA</b>	Wydanie: 3	<b>10.08.2025</b>
			Strona 78 z 81
	<b>POLITYKA OCHRONY DANYCH OSOBOWYCH</b>	Nr dokumentu: <b>7- Pr5</b>	

### Oświadczenie pracowników

.....

(komórka organizacja szpitala - pieczętka)

Oświadczam, że zapoznałem(-am) się z treścią procedury ..... i zobowiązuję się do jej stosowania.

Lp	Nazwisko i imię	Stanowisko	Data	Podpis
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				