Instrukcja nr 6 do
Polityki bezpieczeństwa
danych w systemach
informacyjnych.

Instrukcja kontroli podmiotów przetwarzających

1. Administrator Danych dopuszcza, by dane osobowe, których jest administratorem w rozumieniu art. 4 pkt 7 RODO, były przetwarzane poza jego strukturami organizacyjnymi przez podmioty przetwarzające.
2. Przetwarzanie danych osobowych przez podmioty przetwarzające może się odbywać wyłącznie w określonym celu i zakresie, na mocy umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego.
3. Administrator Danych ma prawo kontroli podmiotów przetwarzających, którym powierzył przetwarzanie danych osobowych z punktu widzenia zgodności tego przetwarzania z: a. przepisami prawa,
   b. postanowieniami zawartej umowy powierzenia przetwarzania danych osobowych,
   c. wytycznymi i rekomendacjami organów nadzorczych oraz organów doradczych w zakresie ochrony danych i prywatności.
4. Kontrola, o której mowa w pkt 3 prowadzona jest w postaci audytu podmiotu przetwarzającego.
5. Szczegóły dotyczące audytu podmiotu przetwarzającego określa zawarta z tym podmiotem umowa powierzenia przetwarzania danych osobowych. W szczególności, dotyczy to postanowień w zakresie sposobu i terminu przekazywania podmiotowi przetwarzającemu informacji o terminie i zakresie audytu.
6. W sytuacji, gdy umowa powierzenia przetwarzania danych osobowych nie określa sposobu i terminu przekazywania podmiotowi przetwarzającemu informacji o terminie i zakresie audytu, kwestie te ustalane są z tym podmiotem w formie porozumienia przed przeprowadzeniem pierwszego audytu, z zastrzeżeniem, że poczynione ustalenia pozostają właściwe dla przyszłych audytów.
7. Audyt podmiotu przetwarzającego może zostać przeprowadzony, w szczególności w następujących przypadkach:
   a. powierzenie przetwarzania obejmuje szczególne kategorie danych osobowych i/lub dane osobowe dotyczące wyroków skazujących oraz naruszeń prawa,
   b. powierzenie przetwarzania obejmuje dane osobowe osób poniżej 16 rż.,
   c. powierza się przetwarzanie danych osobowych na dużą skalę,
   d. Administrator Danych otrzymał informację o incydentach z zakresu ochrony danych osobowych występujących u podmiotu przetwarzającego.
8. Decyzję o przeprowadzeniu audytu podmiotu przetwarzającego podejmuje Administrator Danych po konsultacji z Inspektorem Ochrony Danych:
12. Audyt podmiotu przetwarzającego realizowany jest przez Inspektor Ochrony Danych. Jeżeli jest to zasadne, IOD realizuje audyt przy współpracy z innymi osobami upoważnionymi przez Administratora Danych, których wiedza może mieć kluczowe znaczenie dla merytorycznej poprawności przeprowadzanego audytu.
13. Audyt podmiotu przetwarzającego realizowany jest:
   a. w siedzibie podmiotu przetwarzającego,
   b. w głównym miejscu przetwarzania powierzonych danych osobowych, lub c. zdalnie.
14. Administrator Danych, Inspektor Ochrony Danych opracowują wspólnie harmonogram przeprowadzania audytu, który wskazuje w szczególności na: a. termin audytu,
   b. miejsce audytu,
   c. zakres audytu,
   d. osoby biorące udział w audycie.

15. Inspektor Ochrony Danych, informuje ten podmiot o terminie, miejscu i zakresie audytu.

16. IOD przeprowadza audyt z wykorzystaniem formularza audytu, którego wzór znajduje się w niniejszym Załączniku.
17. Formularz audytu uzupełniany jest:
    a. w przypadku audytu w siedzibie podmiotu przetwarzającego lub w głównym miejscu przetwarzania powierzonych danych osobowych – przez Inspektora Ochrony Danych lub inną osobę do tego wyznaczoną
    b. w przypadku audytu zdalnego – przez osoby upoważnione do tego przez podmiot przetwarzający.
18. Po przeprowadzonym audycie Inspektor Ochrony Danych sporządza Protokół poaudytowy, według wzoru znajdującego się w niniejszym Załączniku.
19. IOD przedkłada Protokół Administratorowi oraz Podmiotowi Przetwarzającemu
20. Podmiot przetwarzający ma 7 dni na ustosunkowanie się do treści przedstawionego mu Protokołu poaudytowego, z zastrzeżeniem, że umowa powierzenia przetwarzania danych osobowych zawarta z tym podmiotem może określać inny termin.
21. Jeżeli w wyniku audytu stwierdzono niezgodność przetwarzania powierzonych danych osobowych z:
    a. obowiązującymi przepisami prawa, lub
    b. postanowieniami zawartej umowy powierzenia przetwarzania danych osobowych,
    c. wytycznymi i rekomendacjami organów nadzorczych oraz organów doradczych w zakresie ochrony danych i prywatności,

    Administrator Danych, na podstawie przedłożonego mu Protokołu poaudytowego, podejmuje ostateczną decyzję w zakresie dalszej współpracy z podmiotem przetwarzającym.
22. Formularz audytu podmiotu przetwarzającego jest stosowany przez Administratora Danych również w stosunku do podmiotów, z którymi Administrator Danych chce nawiązać współpracę tj. potencjalnych podmiotów przetwarzających. W odniesieniu do takich podmiotów, niniejszą Procedurę kontroli podmiotów przetwarzających stosuje się odpowiednio z wyłączeniem pkt 5-6 oraz pkt 21 lit. b

Wzór formularza audytu podmiotu przetwarzającego

FORMULARZ AUDYTU PODMIOTU PRZETWARZAJĄCEGO			
Administrator Danych		**Nazwa:** **Siedziba:**	
Podmiot przetwarzający		**Nazwa:** **Siedziba:**	
Data i miejsce audytu **w przypadku audytu zdalnego należy wskazać datę uzupełnienia Formularza*			
Osoby reprezentujące podmiot przetwarzający biorące udział w audycie **w przypadku audytu zdalnego należy wskazać osoby odpowiedzialne za uzupełnienie Formularza*		1. …*(imię, nazwisko, stanowisko, dane kontaktowe)*… 2. …*(imię, nazwisko, stanowisko, dane kontaktowe)*… 3. …*(imię, nazwisko, stanowisko, dane kontaktowe)*…	
Osoby reprezentujące Administratora Danych biorące udział w audycie **w przypadku audytu zdalnego należy wskazać osoby do których Formularz jest wysyłany*		1. …*(imię, nazwisko, stanowisko, dane kontaktowe)*… 2. …*(imię, nazwisko, stanowisko, dane kontaktowe)*… 3. …*(imię, nazwisko, stanowisko, dane kontaktowe)*…	
Lp.	**Obszar**	**Pytania pomocnicze**	**Stan faktyczny**
1.	**Usługi świadczone na rzecz Administratora Danych**	1. Jaki jest rodzaj usług świadczonych przez podmiot przetwarzający, w związku z którymi dochodzi do powierzenia przetwarzania danych osobowych?	
2.	**Zakres przetwarzanych danych osobowych**	1. Kogo dane osobowe są przetwarzane?	
		2. Czy przetwarzane są dane osób poniżej 16 r.ż.?	
		3. Jakie kategorie danych osobowych są przetwarzane?	
		4. Czy przetwarzane są szczególne kategorie danych? (*jakie*)	
		5. Czy przetwarza się dane dotyczące wyroków skazujących	

		i naruszeń prawa?	

3.	**Struktura organizacyjna**	1. Czy wyznaczono Inspektora Ochrony Danych? (*imię, nazwisko oraz dane kontaktowe*)	
		2. Jeżeli nie wyznaczono IOD, czy wyznaczono osobę o podobnym stanowisku, nadzorującą kwestie związane z ochroną danych osobowych? (*funkcja, imię, nazwisko oraz dane kontaktowe*) 3. Czy wyznaczono osobę odpowiedzialną za zabezpieczenia danych osobowych przetwarzanych za pomocą systemów informatycznych? (*imię, nazwisko, stanowisko oraz dane kontaktowe*)	
4.	**Polityki ochrony danych osobowych**	1. Jakie polityki w zakresie ochrony danych osobowych została wdrożona?	
		2. W jaki sposób polityki ochrony danych osobowych została wdrożona? (*np. formalnie zatwierdzone i wprowadzone w życie procedury dot. środków ochrony danych osobowych*)	
		3. Czy jest przeprowadzana regularna aktualizacja tej polityk ochrony danych osobowych?	
5.	**Audyt**	1. Czy wdrożono program audytowy obejmujący zgodność z regulacjami w zakresie ochrony danych osobowych?	
		2. Jeżeli tak, kto jest odpowiedzialny za przeprowadzanie audytów?	
		3. Jakie są metody przeprowadzania audytów, ich częstotliwość oraz zakres?	
6.	**Incydenty**	1. Czy wdrożono procedurę postępowania z incydentami z zakresu ochrony danych osobowych?	
		2. Czy osoby posiadające dostęp do powierzonych danych osobowych zostali przeszkoleni w zakresie zgłaszania incydentów z zakresu ochrony danych	

		osobowych?	

		3. Czy w okresie ostatnich trzech lat miały miejsce incydenty z zakresu ochrony danych osobowych? (*rodzaj, ilość*)	
		4. Czy w okresie ostatnich trzech lat działalność podmiotu przetwarzającego była przedmiotem postępowania ze strony urzędów zajmujących się ochroną danych osobowych? (*rodzaj, ilość*)	
		5. Czy w okresie ostatnich trzech lat działalność podmiotu przetwarzającego była przedmiotem działań prawnych dotyczących zarzutów naruszenia prywatności lub ochrony danych osobowych? (*rodzaj, ilość*)	
		6. Czy w okresie ostatnich trzech lat podmiot przetwarzający zgłosił jakiekolwiek naruszenia bezpieczeństwa danych odpowiednim organom / urzędom (uwzględniając organy związane z ochroną danych osobowych) oraz / lub podmiotom zajmującym się ochroną danych osobowych?	
		7. Czy podmiot przetwarzający jest zdolny do powiadomienia Administratora Danych o jakimkolwiek naruszeniu bezpieczeństwa, które mogłoby mieć negatywne skutki dla ochrony powierzonych do przetwarzania danych osobowych oraz praw i wolności osób, których te dane dotyczą, bez opóźnienia, tj. w ciągu 24 godzin od chwili powzięcia informacji o naruszeniu?	
7.	**Osoby posiadające dostęp do powierzonych danych osobowych w strukturze podmiotu przetwarzającego**	1. Czy stosuje się politykę lub procedurę ograniczającą dostęp do powierzonych danych osobowych?	
		2. W jaki sposób podejmowane są decyzje o tym, kto powinien otrzymać dostęp do powierzonych danych osobowych i w jaki sposób jest to sprawdzane i potwierdzane?	

		3. Jaka jest forma współpracy z osobami posiadającymi dostęp do powierzonych danych osobowych? (*umowa o pracę, umowa cywilnoprawna, umowa o współpracy*)	
		4. Czy osoby posiadające dostęp do powierzonych danych osobowych odbywają szkolenia w zakresie przetwarzania i ochrony prywatności danych oraz zgodności z przepisami prawa w zakresie ochrony danych osobowych? (*forma szkoleń, częstotliwość*)	
		5. Czy osobom posiadającym dostęp do powierzonych danych osobowych nadawane są upoważnienia do przetwarzania danych osobowych?	
		6. Czy osoby posiadające dostęp do powierzonych danych osobowych składają oświadczenia o zachowaniu tych danych w poufności przez okres trwania współpracy jak i po jej zakończeniu?	
		7. Czy prowadzona jest ewidencja osób posiadających dostęp do powierzonych danych osobowych?	
		8. Czy w przypadku zakończenia współpracy z osobami posiadającymi dostęp do powierzonych danych osobowych, fizyczny i elektroniczny dostęp do powierzonych danych osobowych jest odbierany natychmiast po zakończeniu współpracy? (*sposób odbioru dostępu*)	
8.	**Forma przetwarzania powierzonych danych osobowych**	1. W jakiej formie przetwarzane są powierzone dane osobowe? (*papierowa, elektroniczna*)	
		2. Jeżeli dane osobowe przetwarzane są w formie elektronicznej, za pomocą systemów informatycznych, proszę podać nazwy tych systemów.	
9.		1. W jakich lokalizacjach ma miejsce przetwarzanie powierzonych danych osobowych? (*dane*	

	Miejsce przetwarzania powierzonych danych osobowych	*osobowe przetwarzane na bieżąco, wersje archiwalne, kopie zapasowe*)	
		2. Czy jest prowadzona aktualna ewidencja dotycząca lokalizacji i przemieszczania sprzętu i nośników elektronicznych, które mogą zawierać powierzone dane osobowe?	
10.	**Podpowierzanie powierzonych danych osobowych**	1. Czy powierzone dane osobowe są podpowierzane innym podmiotom?	
		2. Jeżeli tak, jakim podmiotom i w jakim zakresie? (*nazwy podmiotów, zakres danych podpowierzanych poszczególnym podmiotom*)	
		3. Czy z podmiotami, którym podpowierza się dane osobowe zawarto umowę podpowierzenia?	
		4. Czy zawarta umowa podpowierzenia przewiduje nałożenie na podmiot, któremu dane są podpowierzane te same obowiązki ochrony danych jakie zostały nałożone na podmiot przetwarzający na mocy umowy powierzenia z Administratorem Danych?	
		5. Czy podmiot przetwarzający monitoruje lub dokonuje audytu zgodności przetwarzania podpowierzonych danych osobowych z przepisami prawa oraz postanowieniami zawartej umowy podpowierzenia przetwarzania danych osobowych? (*zakres, częstotliwość audytów, metody, odpowiedzialność*)	
		6. Czy w przypadku zakończenia współpracy z podmiotem, któremu dane są podpowierzane, fizyczny i elektroniczny dostęp do powierzonych danych osobowych jest odbierany natychmiast po zakończeniu współpracy? (*sposób odbioru dostępu*)	
11.	**Udostępnianie powierzonych danych osobowych**	1. Czy powierzone dane osobowe są udostępniane innym podmiotom? (*zakres udostępnianych danych, nazwy podmiotów*)	

		2. Jeżeli tak, jakim podmiotom i w jakim zakresie? (*nazwy podmiotów, zakres danych udostępnianych poszczególnym podmiotom*)	
12.	**Przekazywanie powierzonych danych osobowych do państw trzecich**	1. Czy powierzone dane osobowe są przekazywane do państw trzecich?	
		2. Jeżeli tak, do jakich państw trzecich, jakim podmiotom, w jakim zakresie i na jakiej podstawie? (*państwo trzecie, nazwy podmiotów, zakres przekazywanych danych poszczególnym podmiotom, podstawa prawna*)	
13.	**Zabezpieczenia fizyczne**	1. Jakie zabezpieczenia fizyczne wdrożono dla ochrony powierzonych danych osobowych? **Należy opisać wdrożone zabezpieczenia fizyczne, w szczególności to jak zostały zabezpieczone pomieszczenia, w których przetwarzane są powierzone dane osobowe (polityki i procedury dostępu do pomieszczeń, rodzaj drzwi, rodzaj zamków, formy kontroli dostępu, formy zabezpieczenia przed osobami z zewnątrz, monitoring, ochrona, alarm, etc.) oraz to jak przechowuje się nośniki, na których przetwarzane są powierzone dane osobowe (rodzaje szaf, dane osobowe w formie papierowej (rodzaj szaf, zabezpieczenia fizyczne komputerów, niszczarki do dokumentów, etc.)*	
14.	**Zabezpieczenia techniczne**	1. Jakie zabezpieczenia techniczne wdrożono dla ochrony powierzonych danych osobowych? **Należy opisać wdrożone zabezpieczenia techniczne, w szczególności jakie środki wdrożone zostały dla ograniczenia dostępu do powierzonych danych osobowych (kontrola dostępu poprzez ograniczanie uprawnień, indywidualny login i hasło, wymagania dotyczące złożoności hasła, okresowa kontrola uprawnień, etc.), jakie środki techniczne są stosowane do zapewnienia bezpieczeństwa systemu (antywirus, firewall, IPS, IDS, etc.), jakie środki*	

		wdrożone zostały dla zagwarantowania rozliczalności, poufności i integralności powierzonych danych osobowych	
			…….....
			Data i podpis osoby wypełniającej Formularz

Wzór protokołu poaudytowego

PROTOKÓŁ POAUDYTOWY NR …/…….

…….
miejscowość, data

1. Administrator Danych:
   …..……..
2. Podmiot przetwarzający:
   ….……..…….…..……...……..
3. Data rozpoczęcia audytu:
   ……...…….…….
   ……..
4. Data zakończenia audytu:
   ……..…….…….
   ……..
5. Miejsce audytu:
   ……..
   …….
6. Osoby prowadzące czynności audytowe (*imiona, nazwiska, stanowiska*):
   …….……..
7. Osoby upoważnione przez podmiot przetwarzający do udzielania wyjaśnień w trakcie czynności audytowych (*imiona, nazwiska, stanowiska*):
   …….
   ……..
8. Zakres audytu:
   ……..……..
9. Wykaz czynności podjętych w toku audytu:
   ……..……..
10. Wnioski poaudytowe:
    ……..……..

Kluczowe wnioski:

……...……..

Stwierdzone niezgodności przetwarzania powierzonych danych osobowych z obowiązującymi przepisami prawa:

……..

Stwierdzone niezgodności przetwarzania powierzonych danych osobowych z postanowieniami zawartej umowy powierzenia przetwarzania danych osobowych:

……

Stwierdzone niezgodności przetwarzania powierzonych danych osobowych z wytycznymi i rekomendacjami organów nadzorczych oraz organów doradczych w zakresie ochrony danych i prywatności

……
…

Rekomendacje:

…….....
.....
…….....
.....

11. Załączniki:

1) Formularz audytu podmiotu przetwarzającego z dnia …/…/…...

_____

Data i podpis Inspektora Ochrony Danych

Otrzymują:

1 x oryginał Administrator Danych
1 x kopia podmiot przetwarzający
1 x kopia Inspektor Ochrony Danych

Załącznik nr 1 do
Polityki bezpieczeństwa danych w systemach informacyjnych.

UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH NR ……/…….

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO) – nadaję upoważnienie Pani/Panu:

……..……

(imię i nazwisko) zatrudnionej/zatrudnionego/wykonującej/wykonującego obowiązki†:

……..……

(stanowisko/funkcja nazwa jednostki/komórki organizacyjnej) do dostępu i przetwarzania danych osobowych w zakresie i w celu niezbędnym do pełnienia obowiązków służbowych/wykonywania zadań objętych przedmiotem umowy zawartej z Instytutem Matki i Dziecka w tym danych szczególnej kategorii (w szczególności danych medycznych tj. danych dotyczących zdrowia oraz danych genetycznych)† na zajmowanym stanowisku/wykonywania* zadań objętych przedmiotem umowy zawartej z Instytutem Matki i Dziecka. Jednocześnie zobowiązuję Panią/Pana* do przestrzegania zasad ochrony danych osobowych oraz bezterminowego zachowania w tajemnicy danych osobowych przetwarzanych w dokumentach tradycyjnych i systemach informatycznych administratora.

Upoważnienie obowiązuje w okresie zatrudnienia/wykonywania umowy,
Wszystkie dotychczasowe ustne lub pisemne upoważnienia do przetwarzania danych osobowych zastępuje się niniejszym.

Warszawa, dnia …….. ……..……

Pieczęć i podpis Administratora Danych lub upoważnionego przedstawiciela

OŚWIADCZENIE PRACOWNIKA

Ja niżej podpisany/na oświadczam, iż:

2. Zostałam/zostałem* przeszkolona/przeszkolony* w zakresie ochrony danych osobowych, i znana jest mi treść Polityki bezpieczeństwa danych w systemach informacyjnych Instytutu Matki i Dziecka wraz z załącznikami.
3. Zobowiązuję się:
   - do przestrzegania i stosowania zasad zawartych w Polityce bezpieczeństwa danych w systemach informacyjnych,
   - zachować w tajemnicy dane w tym dane osobowe i dane medyczne, do których mam lub będę miał/a dostęp w trakcie wykonywania czynności zleconych przez Pracodawcę zarówno w czasie trwania stosunku pracy (umowy) jak i po jego ustaniu,
   - chronić wszelkie dane osobowe, przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
   - zgłaszania naruszeń zasad ochrony danych osobowych oraz incydentów bezpośredniemu przełożonemu oraz osobom odpowiedzialnych za bezpieczeństwo przetwarzanych danych.

…..……..…..

Data i czytelny podpis pracownika

*niewłaściwe skreślić

Załącznik nr 2 do
Polityki bezpieczeństwa danych w systemach informacyjnych.

Wykaz budynków, stref i pomieszczeń, w których przetwarzane są dane osobowe, których administratorem jest Instytut Matki i Dziecka

Nazwa/numer budynku/strefy/pomieszczenia	Lokalizacja	Uwagi
Budynek A	Ul. Kasprzaka 17a, 01-211 Warszawa	
Budynek B	Ul. Kasprzaka 17a, 01-211 Warszawa	
Budynek C	Ul. Kasprzaka 17a, 01-211 Warszawa	

Załącznik nr 3 do
Polityki bezpieczeństwa danych w systemach informacyjnych.

Wykaz

zbiorów danych osobowych, opis struktury zbiorów danych osobowych wraz z listą systemów informacyjnych oraz sposób przepływu danych pomiędzy poszczególnymi systemami.

W Instytucie Matki i Dziecka dane osobowe przetwarzane są w systemie rozproszonym to znaczy zarówno w systemach kartotekowych (tradycyjnych, papierowych) jak i informatycznych (elektronicznych).

Następujące zbiory danych osobowych, obsługiwane są przez kilka systemów kartotekowych i informatycznych:

1. Zbiór kadrowo-płacowy.
2. Zbiór finansowo-księgowy.
3. Zbiór medyczny.

Ad 1. W zbiorze kadrowo-płacowym przetwarzane są dane osobowe niezbędne ze względu na rozliczenia pracodawcy z pracownikiem oraz z innymi organami państwowymi takimi jak Urzędy Skarbowe, ZUS, Sądy, Komornicy, Ubezpieczyciele wynikające z obowiązujących ustaw i rozporządzeń.

Ad 1a. Dane przetwarzane są w następujących systemach:

- systemy kartotekowe (ewidencja papierowa),
- system informatyczny InfoMedica (moduły kadrowo-płacowe),
- system informatyczny Płatnik,
- system informatyczny bankowości elektronicznej.

Ad 1b. Dane przetwarzane są w następujących polach:

- Imiona,
- Nazwiska,
- Nazwisko Rodowe,
- Pesel,
- Płeć,
- Data Urodzenia,
- Adresy zameldowania, zamieszkania, korespondencyjny,
- Stan Cywilny,
- Stan Zdrowia,
- Zwolnienia, nieobecności i urlopy,
- Wynagrodzenie,
- Przynależność do organizacji związkowych,
- Wykształcenie,
- Świadczenia socjalne, ➢ Szkolenia i delegacje, ➢ Zobowiązania i należności, ➢ Kary i nagrody.

Ad 2. W zbiorze finansowo-księgowym przetwarzane są dane osobowe niezbędne ze względu na rozliczenia pracodawcy z pracownikami i kontrahentami, jak i również z przesyłaniem wynagrodzenia, składek na rzecz innych organizacji, rozliczeń zaliczek, pożyczek i świadczeń socjalnych, jak również rozliczeń w ramach pracowniczej kasy zapomogowo pożyczkowej, podróży służbowych, szkoleń, egzekwowania należności, spłat zobowiązań.

Ad 2a. Dane przetwarzane są w następujących systemach:

- systemy kartotekowe (ewidencja papierowa),
- system informatyczny InfoMedica (moduły finansowy, księgowy, kasowy, pożyczkowy),
- system informatyczny bankowości elektronicznej.

Ad 2b. Dane przetwarzane są w następujących polach:

- Imiona,
- Nazwiska
- Pesel,
- Data urodzenia,
- Adres zamieszkania,
- Stawki odprowadzane na rzecz innych organizacji w tym (ubezpieczenie, izba lekarska, PKZP, świadczenia socjalne, wypłacone zaliczki, rozliczenia zaliczek, rozliczenia delegacji, ściągane należności).

Ad 3. W zbiorze medycznym przetwarzane są dane osobowe i dane medyczne, będące danymi wrażliwymi, niezbędne do prowadzenie procesu leczenia pacjenta jak i rozliczenia Instytutu Matki i Dziecka za wykonane świadczenia medyczne.

Ad 3a. Dane przetwarzane są w następujących systemach

- systemy kartotekowe (ewidencja papierowa),
- kompleksowy system informatyczny CliniNet (moduły izby przyjęć, oddziału, rejestracji, gabinetu lekarskiego, gabinetu diagnostycznego, pracowni)
- systemy informatyczne rozliczeniowe (moduł rozliczeniowy CliniNet – STER, moduł rozliczeniowy PPS, moduł rozliczeniowy diagnostyki obrazowej Schomberg),
- system informatyczny laboratoryjny (moduł laboratoryjny CliniNet, system laboratoryjny w Zakładach Immunologii, Badań Przesiewowych, Genetyki Medycznej),
- system informatyczny diagnostyki obrazowej (moduł obrazowy CliniNet, system obrazowy firmy Siemens).

Ad 3b. Dane przetwarzane są w następujących polach

- Imiona,
- Nazwiska,
- Płeć,
- Pesel,
- Data urodzenia,
- Adres zamieszkania,
- Ubezpieczyciel,
- Rozpoznania,
- Przebieg dotychczasowego leczenia,
- Badania i wyniki badań diagnostycznych i laboratoryjnych wykonanych przed i w trakcie procesu leczniczego,
- Przeprowadzone zabiegi i operacje oraz ich wyniki,
- Przebieg choroby,
- Dane genetyczne,
- Zalecenie lekarskie,

- Zwolnienia,
- Dane rozliczeniowe z NFZ, ministerstwem zdrowia i innymi jednostkami medycznymi i niemedycznymi.

Dane pomiędzy poszczególnymi wewnętrznymi systemami i zbiorami wymieniane są zarówno drogą elektroniczną jak i papierową, z zachowaniem komunikacji dwustronnej. Z instytucjami zewnętrznymi zbiory i systemy wymieniają dane zarówno drogą elektroniczną jak i papierową, w zależności od możliwości poszczególnych systemów, z zachowaniem komunikacji dwustronnej, o ile taka komunikacja jest możliwa. Przekazywane są tylko dane niezbędne dla celów identyfikacji osób i rozliczenia tych osób z wykonanych usług, zadań, prac oraz wykonania obowiązków nałożonych na Instytut Matki i Dziecka przez organy państwowe.

Załącznik nr 4 do
Polityki bezpieczeństwa danych w systemach informacyjnych.

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH w Instytucie Matki i Dziecka (wzór)

Lp.	Nazwa bazy danych	Nazwisko	Imię	Rodzaj uprawnień	Numer upoważnienia	Nazwa identyfikatora	Data		Jednostka/ Komórka organizacyjna	Uwagi	Telefon	Okres upoważnienia	Stanowisko
							Nadania uprawnień	Ustania uprawnień					
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**

Legenda:

1) Kolumna 5 – wpisać skróty stosowane do określenia uprawnień w systemie informatycznym:

P - pełne prawa do zarządzania bazą danych;

W - pełne prawa do edycji danych (w tym drukowania, archiwizowania, usuwania);

N - prawo do zakładania nowych kont;

C - prawo do tworzenia nowych danych;

M - prawo modyfikacji istniejących danych;

O - prawo do odczytu danych;

D - prawo do drukowania danych;

A - prawo do wykonywania kopii archiwalnych;

3) **E** - skrót stosowany do określenia uprawnień poza systemem informatycznym.

Uwaga: w przypadku praw ograniczonych do określonej części bazy danych (np. stażystów, wolontariuszy itp.) należy ograniczenie to podać w polu Uwagi

Załącznik nr 5 do
Polityki bezpieczeństwa danych w systemach informacyjnych.

EWIDENCJA UDOSTĘPNIEŃ/POWIERZEŃ DANYCH OSOBOWYCH przetwarzanych w Instytucie Matki i Dziecka (wzór)

Lp.	Nazwa i adres odbiorcy danych/podmiot któremu powierzono dane	Podstawa udostępnienia/powierzenia	Data udostępnienia/powierzenia	Zakres i cel udostępnienia/powierzenia danych	Uwagi
1	2	3	4	5	6

Rejestr czynności przetwarzania (wzór)

Administrator: Instytut Matki i Dziecka 01-211 Warszawa, ul. Kasprzaka 17A
Inspektor Ochrony Danych: (imię i nazwisko) e-mail: iod@imid.med.pl numer telefonu: 22 32 77 394

Nr	Czynności i cele przetwarzania	Kategorie osób, których dane dotyczą	Kategorie danych osobowych	Kategorie odbiorców	Transfer do państw trzecich	Termin usunięcia danych	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa	Źródło danych	Podstawa przetwarzania
1.									
2.									
3.									

Załącznik nr 6 do
Polityki bezpieczeństwa danych w systemach informacyjnych.

Rejestr kategorii czynności przetwarzania (wzór)

Podmiot przetwarzający: (pełne dane podmiotu przetwarzającego)
Inspektor Ochrony Danych: (imię i nazwisko) e-mail: iod@imid.med.pl numer telefonu: 22 32 77 394

Nr	Administrator	Kategorie przetwarzań dokonywanych w imieniu administratora	Transfer do państw trzecich	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa
1.				
2.				
3.				

Załącznik nr 7 do
Polityki bezpieczeństwa danych w systemach informacyjnych.

Ewidencja naruszeń (wzór)

Administrator: Instytut Matki i Dziecka, 01-211 Warszawa ul. Kasprzaka 17A
Inspektor Ochrony Danych: (imię i nazwisko)

Numer naruszenia	Opis naruszenia	Data i godzina zgłoszenia do UODO	Data zawiadomienia osoby (osób), której (których) dane dotyczą	Data i godzina stwierdzenia naruszenia	Data i godzina powstania naruszenia (jeśli jest to możliwe)	Kategorie oraz liczba osób, których naruszenie dotyczy	Zakres danych, których dotyczy naruszenie	Opis skutku/konsekwencji naruszenia	Środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.	Prawdopodobieństwo naruszenia praw i wolności osób, których dane dotyczą
1.										