**Polityka Ochrony Danych Osobowych w Powiatowym Centrum Pomocy Rodzinie w Lubaczowie**

Na podstawie art. 24 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

**ustala się, co następuje:**

**Wstęp**

Niniejszy dokument jest Polityką ochrony danych osobowych w rozumieniu RODO - Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1).

**§ 1**

**Cel i zakres polityki:**

1. Celem Polityki jest przedstawienie zasad ochrony danych osobowych obowiązujących w Powiatowym Centrum Pomocy Rodzinie w Lubaczowie.
2. Zakres przedmiotowy stosowania obejmuje wszystkie procesy przetwarzania danych osobowych w Powiatowym Centrum Pomocy Rodzinie w Lubaczowie, zarówno w formie elektronicznej jak i papierowej.
3. Zakres podmiotowy obowiązuje wszystkich pracowników Powiatowego Centrum Pomocy Rodzinie w Lubaczowie, oraz inne osoby świadczące prace na rzecz Powiatowego Centrum Pomocy Rodzinie w Lubaczowie upoważnione do przetwarzania danych osobowych.
4. Polityka ochrony uwzględnia:
   1) przepisy RODO,
   2) przepisy krajowe w zakresie ochrony danych osobowych,
   3) akty prawa wewnętrznego obowiązujące w Powiatowym Centrum Pomocy Rodzinie w Lubaczowie,
5. W celu uszczegółowienia Polityki ochrony w Powiatowym Centrum Pomocy Rodzinie w Lubaczowie mogą zostać opracowywane i wdrożone procedury, instrukcje i wytyczne dotyczące zidentyfikowanych procesów przetwarzania danych osobowych.

**§ 2**

**Skróty i definicje**

Słownik pojęć i definicji używanych w tym dokumencie:

1. **Polityka** lub **PODO** oznacza niniejszą Politykę ochrony danych osobowych,
2. **RODO** oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1),
3. **Dane** oznaczają **dane osobowe** - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej,
4. **Szczególne kategorie danych osobowych** oznaczają dane specjalne i dane karne,
5. **Dane specjalne** oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej,
6. **Dane karne** oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa,
7. **Osoba** oznacza osobę fizyczną, której dane dotyczą.
8. **Przetwarzający / Podmiot przetwarzający** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora,
9. **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,
10. **Przetwarzanie** oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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,
11. **Pseudonimizacja** oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej,

12. **Anonimizacja** oznacza proces przetworzenia danych osobowych prowadzący do nieodwracalnego braku możliwości identyfikacji osoby, której dane dotyczą,
13. **Eksport danych** oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej,
14. **Organ nadzorczy** oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51; (Prezes Urzędu Ochrony Danych Osobowych).
15. **IOD** lub **Inspektor** oznacza Inspektora Ochrony Danych w Powiatowym Centrum Pomocy rodzinie w Lubaczowie,
16. **KSI** - oznacza osobę odpowiedzialną za system informatyczny jeżeli jest powołana ,
17. **Rejestr** oznacza Rejestr Czynności Przetwarzania Danych Osobowych w Powiatowym Centrum Pomocy Rodzinie w Lubaczowie,
18. **PCPR** – oznacza Powiatowe Centrum Pomocy Rodzinie w Lubaczowie - urząd, przy pomocy którego PCPR wykonuje zadania,
19. **IZSI -** instrukcja zarządzania bezpieczeństwem systemów informatycznych w Powiatowym Centrum Pomocy Rodzinie w Lubaczowie ,
20. **Administrator** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania,
21. **Odbiorca** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania,
22. **Pracownik** oznacza osobę fizyczną zatrudnioną w Powiatowym Centrum Pomocy Rodzinie w Lubaczowie na podstawie stosunku pracy lub wykonującą umowę zlecenia lub inną umowę cywilno-prawną wymagającą dostępu do danych osobowych np. eksperta wykonującego pracę przy ocenie projektów; a także stażystę, praktykanta pracującego pod nadzorem wyznaczonego opiekuna, jeżeli program stażu, praktyki obejmuje wykonywanie zadań związanych z dostępem do danych osobowych,
23. **Współpracownik** oznacza osobę której zadania, dotyczące przetwarzania danych osobowych zostały określone w dokumentach dotyczących nawiązania współpracy mogą to być np. osoby zatrudnione w innych podmiotach a świadczące pracę na rzecz Powiatowego Centrum Pomocy Rodzinie w Lubaczowie, które w ramach swoich obowiązków służbowych uzyskują dostęp do danych osobowych przetwarzanych w Powiatowym Centrum Pomocy Rodzinie w Lubaczowie (jeśli charakter świadczonych usług przez podmiot nie wpisuje się w tryb powierzenia przetwarzania danych),
24. **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,
25. **Podmiot danych** oznacza, osobę której dane są przetwarzane,

26. **Naruszenie ochrony danych osobowych** oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych,
27. **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,
28. **Dane genetyczne** oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej,
29. **Dane biometryczne** oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne,
30. **Dane dotyczące zdrowia** oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej - w tym o korzystaniu z usług opieki zdrowotnej - ujawniające informacje o stanie jej zdrowia.

**§3**

**Zarządzanie bezpieczeństwem danych osobowych**

1. Za bezpieczeństwo danych osobowych przetwarzanych w PCPR w tym za wdrożenie i utrzymanie niniejszej Polityki odpowiedzialny jest Administrator , który w myśl przepisów RODO, jako Administrator/Przetwarzający/Współadministrator obowiązany jest zastosować środki techniczne i organizacyjne zapewniające stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia przy uwzględnieniu stanu wiedzy technicznej, kosztu wdrożenia oraz charakteru, zakresu, kontekstu i cele przetwarzania, z zastrzeżeniem ust. 2.
2. Administratorem danych osobowych przetwarzanych w PCPR jest Dyrektor. Podmiot powyższy stosuje zasady przetwarzania danych osobowych określone w niniejszej Polityce oraz innymi dokumentami wdrożonymi w PCPR w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych.
3. Za nadzór i monitorowanie przestrzegania Polityki odpowiadają:
   1) Inspektor Ochrony Danych wyznaczony przez Dyrektora,
   2) Koordynator Systemu Informacyjnego – osoba odpowiedzialna za funkcjonowanie systemu informatycznego, wyznaczona przez Administratora.
4. Za stosowanie niniejszej Polityki odpowiedzialni są pracownicy, których zadania dotyczą przetwarzania danych osobowych,
5. Pracownicy których zadania dotyczą przetwarzania danych osobowych są odpowiedzialni za zapewnienie prawidłowego przetwarzania danych osobowych, w ramach zajmowanych stanowisk ponadto zobowiązani są do:
   1) współdziałania z IOD w sprawach związanych z bezpieczeństwem danych osobowych,

2) wdrożenia w ramach zajmowanych stanowisk rozwiązań organizacyjnych i technicznych umożliwiających skuteczne realizowanie „obowiązku informacyjnego" wynikającego z RODO,
3) podejmowania odpowiednich środków, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14 RODO (Klauzule informacyjne) oraz prowadzić z nią wszelką komunikację na mocy art. 15-22 i 34 RODO w sprawie przetwarzania. Informacji udziela na piśmie lub w inny sposób, w tym w stosownych przypadkach - elektronicznie,
4) jeżeli zgodność przetwarzania danych opiera się na zgodzie wyrażonej przez osobę, której dane dotyczą pracownik jest zobowiązany za posiadanie w formie pisemnej lub elektronicznej zgody z uwzględnieniem określonego celu lub celów przetwarzania i prowadzi rejestr zgód. (Załącznik Nr 1 - Klauzula zgody na przetwarzanie danych osobowych i informacja o prawie do jej cofnięcia),
5) współpracy z KSI i IOD w celu opracowania analizy ryzyka na podległym stanowisku, poprzez opis planowanych operacji, identyfikację zagrożeń i wartości strat, oraz jeżeli jest to możliwe zapobiegania tym zagrożeniom,
6) oceny skutków czynności przetwarzania dla ochrony danych oraz ich wpływu na naruszenia praw lub wolności osób fizycznych,
7) dopełnienia obowiązku uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych,
8) powiadamiania IOD o przypadkach naruszenia ochrony danych osobowych nie później niż 24 godz. od stwierdzenia naruszenia (Załącznik Nr 13 - Wzór Raportu o naruszeniu danych osobowych),
9) przedkładania aktualizacji „Rejestru czynności przetwarzania" lub/i „Rejestru kategorii czynności" dla zbiorów zidentyfikowanych w PCPR według wzorów załączonych do PODO, przesyłanie pisemne i na e-mail do IOD (Załącznik Nr 2, 3) niezwłocznie po wystąpieniu zmian w zbiorze bądź odnotowaniu nowego zbioru. Rejestry podpisuje IOD, (Załącznik Nr 2 - Wzór Rejestru czynności przetwarzania i Załącznik Nr 3 - Rejestr kategorii czynności),
10) dokonywania weryfikacji - przed wyborem podmiotu przetwarzającego, czy gwarantuje odpowiednie środki techniczne i organizacyjne dające możliwość spełnienia wymogów RODO,
11) sporządzania umów (porozumień) powierzenia przetwarzania danych osobowych (w tym zawieranie zapisów dotyczących celu i zakresu przetwarzania, stosowania - zabezpieczeń określonych w RODO z podmiotami zewnętrznymi oraz kontrolowanie ich wykonania,
12) aktualizacji „Ewidencji osób upoważnionych do przetwarzania danych osobowych" według Załącznika Nr 5, a następnie przedkładanie i przesyłanie jej do IOD niezwłocznie po wystąpieniu zmian,
13) opracowanie dodatkowych procedur przetwarzania danych osobowych, nie ujętych w niniejszym dokumencie, ze względu na specyfikę zakresu działania PCPR, które będą obowiązywały po konsultacji z IOD i wprowadzeniu przez AD,
14) w przypadku zawarcia umów powierzenia, gdzie występujemy jako podmiot przetwarzający (procesor) pracownicy zobowiązani są do wykonania obowiązków

nałożonych umowami (np. powiadamiania o incydencie, wykonanie praw osób, których dane dotyczą),

15) sporządzanie umów o współadministrowaniu oraz wykonywanie obowiązków nałożonych tymi umowami,
16) ewidencjonowanie przypadków udostępniania danych osobowych,
17) jeżeli w PCPR wystąpi przetwarzanie danych dziecka wyłącznie dla celów społeczeństwa informacyjnego i w oparciu o zgodę to pracownik postępuje zgodnie zapisami w § 5 ust 1. pkt 6,
18) wyznaczenia pracowników, który współpracuje z IOD w zakresie realizowanych przez PCPR zadań dotyczących ochrony danych osobowych.

6. **Inspektor Ochrony Danych (IOD)** wyznaczony przez Dyrektora, podlega bezpośrednio Dyrektorowi i realizuje w PCPR zadania dotyczące:
   1) informowania administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tym zakresie,
   2) monitorowania przestrzegania RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych oraz 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,
   3) nadzorowania opracowania, wdrożenia i aktualizowania zasad zawartych w dokumentacji określającej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę tych danych,
   4) zapewnienia zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
   5) udzielania na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania,
   6) współpracy z organem nadzorczym,
   7) pełnienia funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,
   8) pełnienia roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia,
   9) prowadzenia zbiorczego rejestru czynności lub/i rejestru kategorii czynności w imieniu administratora,
7. Koordynator Systemu informatycznego (KSI), wyznaczany jest przez Dyrektora lub osobę przez niego upoważnioną. W ramach ochrony przetwarzanych danych osobowych w PCPR, koordynuje i nadzoruje realizację zadań zapewniających prawidłowe funkcjonowanie systemów teleinformatycznych, w których przetwarzane są dane osobowe. Wraz z IOD prowadzi rejestr naruszeń danych osobowych według załącznika Nr 12 do Polityki.

**§4**

**Zasady ochrony danych**

W PCPR przetwarza się dane osobowe z poszanowaniem następujących zasad:

1. w oparciu o podstawę prawną i zgodnie z prawem (legalizm - art.6, 9 RODO),
2. rzetelnie i uczciwie (rzetelność),
3. w sposób przejrzysty dla osoby, której dane dotyczą (transparentność),
4. w konkretnych celach i nie „na zapas" (celowość, ograniczenie celu),
5. gromadzenie nie więcej niż potrzeba (adekwatność, minimalizacja danych),
6. z dbałością o prawidłowość danych (prawidłowość),
7. nie dłużej niż potrzeba (czasowość),
8. zapewniając odpowiednie bezpieczeństwo danych (integralność i poufność),
9. dokumentując czynności przetwarzania (rozliczalność),
10. umożliwiając realizację przez osoby, których dane są przetwarzane, swoich praw zgodnie z obowiązującymi przepisami prawa (ochrona prywatności osób fizycznych).

**§5**

**System ochrony danych osobowych**

System ochrony danych osobowych przetwarzanych w PCPR składa się z następujących zasadniczych elementów:

1. Inwentaryzacja danych:
   1) Dane osobowe wymagające ochrony zostały wykazane w wykazie zbiorów. Wykaz obejmuje zbiory ze stwierdzonym potencjalnym ryzykiem naruszenia praw lub wolności osób fizycznych. Każdy ze zbiorów jest opisany w sposób umożliwiający przeprowadzenie analizy ryzyka,
   2) Opis zbiorów obejmuje takie informacje, jak:
      a) nazwę zbioru,
      b) opis celów przetwarzania,
      c) charakter, zakres, kontekst, rodzaj danych (dane zwykłe, dane szczególne),
      d) odbiorcy,
      e) podstawę prawną przetwarzania danych osobowych,
      f) funkcjonalny opis operacji przetwarzania,
      g) aktywa służące do przetwarzania danych osobowych (ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, programy, systemy operacyjne, informacja o powierzeniu danych osobowych, informacja o wykonywaniu usług przez podmioty zewnętrzne, źródła pochodzenia danych osobowych),
   3) Szczególne kategorie danych osobowych. Identyfikacja przypadków, w których przetwarza lub może przetwarzać szczególne kategorie danych osobowych (dane specjalne i dane karne) oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności

z prawem przetwarzania takich danych. Weryfikuje podstawy prawne przetwarzania takich danych w oparciu o art. 9 i art. 10 RODO oraz zapewnienia szczególnej ochrony przetwarzania tych danych,

4) Dane niezidentyfikowane. Identyfikacja przypadków, w których przetwarza lub może przetwarzać dane niezidentyfikowane i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane. Administrator nie odmawia przyjęcia dodatkowych informacji od osoby, której dane dotyczą by ułatwić jej wykonanie jej praw i w takim przypadku dokonuje weryfikacji tożsamości np. poprzez mechanizmy uwierzytelniania,
5) Profilowanie. Identyfikacja przypadków, w których dokonuje się profilowania przetwarzanych danych i utrzymuje mechanizmy zapewniające zgodność tego procesu z prawem. W przypadku zidentyfikowania przypadków profilowania i w pełni zautomatyzowanego podejmowania decyzji, Administrator informuje osobę, której dane dotyczą o fakcie profilowania oraz o konsekwencjach takiego profilowania. Jeżeli gromadzi jej dane informuje ją również czy ma ona obowiązek podać te dane oraz o konsekwencjach ich niepodania. Informację można przekazać w połączeniu ze standardowymi znakami graficznym, które w widoczny, zrozumiały i czytelny sposób przedstawiają sens zamierzonego przetwarzania,
6) Przetwarzanie danych dzieci - stosuje przepisy art.8 RODO. Zgodnie z art. 8 ust. 1 RODO w sytuacji, w której przetwarzanie danych odbywa się na podstawie zgody i dotyczy usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku poniżej 16 roku życia, wymagana jest zgoda udzielona lub zaaprobowana przez osobę sprawującą władzę rodzicielską nad dzieckiem lub opiekę.
   Kluczowe jest zatem, aby przetwarzanie:
   a) odbywało się na podstawie zgody,
   b) dotyczyło wyłącznie usług społeczeństwa informacyjnego,
   c) oferowanych bezpośrednio dziecku w wieku poniżej 16 roku życia,

   Realizacja wymogów wynikających z art. 8 RODO jest związana z nałożonym na administratora obowiązkiem weryfikacji wieku. Administrator wprowadza odpowiednie mechanizmy, uwzględniając dostępną technologię i podejmując racjonalne starania, aby zweryfikować, czy odpowiednia osoba udzieliła zgody lub ją zaaprobowała (komunikacja pocztą tradycyjną lub elektroniczną, zgodę pisemną, inne metody autoryzacyjne),

7) Współadministrowanie. W przypadku gdy Administrator określa cele i sposoby przetwarzania wspólnie z innymi podmiotami może dojść między nimi do zawarcia umowy o współadministrowaniu. W takim przypadku przepis art. 26 ust. 1 RODO nakłada na nich jako na współadministratorów obowiązek określenia, w drodze uzgodnień, w przejrzysty sposób odpowiednich zakresów obowiązków. W szczególności powinno zostać określone, który z współadministratorów będzie realizował obowiązki informacyjne i inne obowiązki wynikające z przepisów RODO. W uzgodnieniach może zostać również wskazany punkt kontaktowy dla osób, których dane dotyczą. Zgodnie z przepisem art. 26 ust. 2 RODO zasadnicza treść uzgodnień powinna zostać udostępniona osobom, których dane dotyczą. Ocena w tym zakresie pozostawiona została współadministratorom. Należy przyjąć, że zasadniczy charakter będą miały co najmniej te uzgodnienia, które odnoszą się do podziału obowiązków między współadministratorami

oraz sposobu realizacji uprawnień podmiotów danych. Dokonanie uzgodnień między współadministratorami nie zwalnia ich z obowiązków przewidzianych przepisami RODO. Ponadto niezależnie od uzgodnień, osoba, której dane dotyczą, może wykonywać przysługujące jej prawa wynikające z RODO wobec każdego z administratorów.

2. Upoważnienia:
   1) Administrator odpowiada za nadawanie / anulowanie upoważnień do przetwarzania danych w zbiorach papierowych, systemach informatycznych,
   2) Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisu prawa,
   3) Upoważnienia nadawane są w formie pisemnej (dopuszcza się formę elektroniczną) w postaci skierowanego imiennie dokumentu do osoby upoważnionej. Minimalne wymagania co do treści upoważnienia zawarte są w Załączniku Nr 4 - Wzór upoważnienia do przetwarzania danych osobowych,
   4) Upoważnienia mogą być nadawane w formie pisemnych poleceń, np. upoważnienia do przeprowadzenia kontroli, audytów, wykonania czynności służbowych, udokumentowanego polecenia administratora w postaci umowy powierzenia,
   5) Osobę, która po raz pierwszy ma mieć dostęp do przetwarzania danych osobowych można upoważnić po zapoznaniu jej z obowiązującą w PCPR Polityką oraz przepisami dotyczącymi ochrony danych osobowych. Szkolenie przeprowadza IOD. Po odbyciu szkolenia osoba ta, podpisuje oświadczenie o zapoznaniu z przepisami dotyczącymi ochrony danych osobowych, zachowaniu w tajemnicy przetwarzanych danych osobowych oraz sposobów ich zabezpieczenia (Załącznik Nr 6 - Oświadczenie o poufności)
   6) Nazwa zbioru/zbiorów przetwarzania musi być zgodna z nazwą zbioru występującą w rejestrze czynności przetwarzania prowadzonym przez IOD,
   7) Podpisane oświadczenie jest przechowywane w teczce osobowej pracownika PCPR.
   8) W przypadku osób, które nie są pracownikami PCPR na podstawie umowy o pracę, dokumenty wymienione w pkt. 5 (powyżej) są dołączane do dokumentacji określającej zakres współpracy i świadczeń wykonywanych na rzecz PCPR przez te osoby lub mogą stanowić jej część,
   9) Zakres upoważnienia może dodatkowo zostać uszczegółowiony w dokumentach określających obowiązki osób wykonujących czynności przetwarzania danych osobowych w PCPR lub na jego rzecz,
   10) Szczegółowy zakres oraz poziom uprawnień do przetwarzanych danych osobowych może zostać dodatkowo określony, w zależności od formy współpracy z PCPR w:
      a) zakresie czynności pracownika oraz opisie dodatkowych zadań wykraczających poza zakres obowiązków pracownika, które są przez niego realizowane,
      b) planie stażu/praktyki,
      c) zawartej umowie cywilno-prawnej,
      d) indywidualnym formularzu dostępu do systemów teleinformatycznych,
   11) Inspektor wraz z pracownikiem PCPR prowadzi ewidencję osób upoważnionych (Załącznik Nr 5 - Ewidencja osób upoważnionych do przetwarzania danych osobowych), w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych. Ewidencję sporządza/aktualizuje po otrzymaniu częściowych ewidencji

prowadzonych w PCPR, które będą przekazywane przez administratora natychmiast po wystąpieniu zmian,

3. Podstawy prawne:
   1) zapewnienie, identyfikowanie, weryfikowanie podstaw prawnych przetwarzania danych i rejestrowanie ich w Rejestrze, w tym:
      a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów. Jeżeli zbierane jest kilka zgód dotyczących różnych celów przetwarzania, zgody te muszą zostać wyrażone osobno. Niedozwolone jest zbiorcze zbieranie zgód,
      b) 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,
      c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze,
      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 administratorowi,
   2) Prawnie uzasadniony interes administratora nie powinien mieć zastosowania jako podstawa prawna przetwarzania, gdyż jako organ publiczny dokonuje tego realizując swoje zadania określone przez ustawodawcę,
4. Eksport danych
   Administrator weryfikuje czy nie przekazuje danych do państw trzecich (czyli poza UE, Norwegię, Lichtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków takiego przekazywania, jeśli ma ono miejsce,
5. Rejestr Czynności Przetwarzania Danych:
   1) Administrator opracowuje, prowadzi i utrzymuje Rejestr czynności przetwarzania danych, zwany „Rejestrem” (Załącznik Nr 2) oraz „Rejestr kategorii czynności" (Załącznik Nr 3) jako podmiot przetwarzający - procesor w przypadku powierzenia danych osobowych,
      a) Rejestr stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności,
      b) IOD prowadzi „Rejestr Czynności Przetwarzania Danych" oraz „Rejestr Kategorii Czynności" w imieniu Administratora, Procesora, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe. Wypełnia rejestry (Załącznik Nr 2 i Nr 3) po otrzymaniu rejestrów czynności przetwarzania danych prowadzonych przez pracowników,
      c) Rejestr czynności prowadzony jest dla każdego zbioru danych osobowych/czynności przetwarzania występującego w PCPR,
      d) Rejestr jest jednym z podstawowych narzędzi umożliwiających rozliczanie większości obowiązków ochrony danych,
      e) Wzór Rejestru stanowi Załącznik nr 2 do Polityki - „Wzór Rejestru Czynności Przetwarzania”. Wzór Rejestru zawiera także kolumny nieobowiązkowe. W

kolumnach nieobowiązkowych rejestruje się informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść Rejestru ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej,

f) Rejestry czynności przetwarzania danych mają charakter dokumentów wewnętrznych i z uwagi na zawarte tam informacje odnoszące się do zabezpieczeń nie mogą być udostępniane osobom nieuprawnionym.

**§6**

**Prawa osoby, której dane dotyczą**

1. Obsługa praw jednostki. Administrator spełnia obowiązki informacyjne względem osób których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
   1) Obowiązki informacyjne. Administrator przekazuje osobom prawem wymagane informacje przy zbieraniu danych oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków,
   2) Możliwość wykonania żądań. Administrator weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających,
   3) Obsługa żądań. Administrator zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO i dokumentowane. Umożliwia wnoszenie przedmiotowych żądań także drogą elektroniczną,
   4) Zawiadamianie o naruszeniach. Administrator stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.
2. Sposób obsługi praw jednostki i obowiązków informacyjnych,
   1) Informacje podawane na mocy art.13 i 14 RODO oraz komunikacja i działania podejmowane na mocy art. 15-22 i 34 RODO są wolne od opłat z zastrzeżeniem ust 4 pkt. 5 niniejszego paragrafu. Administrator dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza,
   2) Administrator ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczenie na stronie internetowej PCPR informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich, metodach kontaktu z Administratorem w tym celu, ewentualnym cenniku żądań „dodatkowych" itp.,
   3) Administrator dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób,
   4) Administrator wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych. Np. takie same dane uwierzytelniające, których osoba, której dane dotyczą użyła, by zalogować się do usług internetowych oferowanych przez administratora,
   5) W celu realizacji praw jednostki Administrator zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzanych, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany,
   6) Administrator dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

3. Obowiązki informacyjne: Załącznik Nr 7 zawiera wzory - Podstawowe klauzule informacyjne (art.13, 14 RODO).
   Administrator:
   1) określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych,
   2) informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby,
   3) informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby, gdy przepis szczegółowy nie stanowi inaczej,
   4) informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej, gdy przepis szczegółowy nie stanowi inaczej,
   5) określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym).
   6) informuje osobę o planowanej zmianie celu przetwarzania danych,
   7) informuje osobę przed uchyleniem ograniczenia przetwarzania,
   8) informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe),
   9) informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą, w przypadku gdy prawo to jej przysługuje,
   10) bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.
4. Żądania osób:
   1) Prawa osób trzecich. Realizując prawa osób, których dane dotyczą, Administrator gwarantuje ochronę praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnicę handlową, dobra osobiste itp.), Administrator może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu,
   2) Nieprzetwarzanie. Administrator informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw,
   3) Odmowa. Administrator informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych,
   4) Dostęp do danych. Na żądanie osoby dotyczące dostępu do jej danych, Administrator informuje osobę, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych, z zastrzeżeniem, że kopii danych wydanej w wykonaniu prawa dostępu do danych, nie uzna się za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych,
   5) Kopie danych. Na żądanie wydaje się osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Administrator odrębnym zarządzeniem może wprowadzać cennik kopii danych, zgodnie z którym pobiera opłaty za kolejne kopie

danych zgodnie z art. 15 ust. 3 RODO. Cena kopii danych skalkulowana jest w oparciu o oszacowany jednostkowy koszt obsługi żądania wydania kopii danych,

6) Sprostowanie danych. Administrator dokonuje sprostowania nieprawidłowych danych na żądanie osoby. Ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby,
7) Uzupełnienie danych. Administrator uzupełnia i aktualizuje dane na żądanie osoby, ma prawo odmówić uzupełnienia lub aktualizacji danych, jeżeli uzupełnienie lub aktualizacja byłoby niezgodne z celami przetwarzania danych. Administrator może polegać na oświadczeniu osoby, co do uzupełnianych lub aktualizowanych danych, chyba że będzie to niewystarczające w świetle prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne,
8) Usunięcie danych. Na żądanie osoby, Administrator usuwa dane, gdy:
    a) dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,
    b) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
    c) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
    d) dane były przetwarzane niezgodnie z prawem,
    e) konieczność usunięcia wynika z obowiązku prawnego,
    f) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. udział w konkursie na stronie internetowej),
    oraz
    g) Administrator określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17. ust. 3 RODO,
    h) W sytuacji gdy przepisy prawa nakładają obowiązek, do którego spełnienia konieczne jest przetwarzanie danych, Administrator nie ma obowiązku spełnienia żądania osoby, której dane dotyczą, odnoszącego się do usunięcia jej danych,
    i) Jeżeli dane podlegające usunięciu zostały upublicznione przez Administratora, podejmuje on rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, o potrzebie usunięcia danych i dostępu do nich,
    j) W przypadku usunięcia danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby,
9) Ograniczenie przetwarzania. W trakcie ograniczenia przetwarzania Administrator przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że 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. Administrator informuje osobę przed uchyleniem ograniczenia przetwarzania. W przypadku ograniczenia przetwarzania danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.

Administrator dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:

a) osoba kwestionuje prawidłowość danych - na okres pozwalający sprawdzić ich prawidłowość,
b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
c) Administrator nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
d) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją - do czasu stwierdzenia, czy po stronie Administrator zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu,

10) Przenoszenie danych. Na żądanie osoby Administrator wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Administratorowi, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Administratora,
11) Sprzeciw w szczególnej sytuacji. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Administratora w oparciu o powierzone zadanie w interesie publicznym, Administrator uwzględni sprzeciw, o ile nie zachodzą po stronie Administratora ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń,
12) Sprzeciw przy badaniach naukowych, historycznych lub celach statystycznych. Jeżeli Administrator prowadzi lub przetwarza dane w celach statystycznych, osoba może wnieść umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania. Administrator uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym,
13) Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu. Jeżeli Administrator przetwarza dane w sposób wyłącznie zautomatyzowany, w tym w szczególności profiluje osoby, i w konsekwencji podejmuje względem osoby decyzje wywołujące skutki prawne lub inaczej istotnie wpływające na osobę, Administrator zapewnia możliwość odwołania się do interwencji i decyzji człowieka po stronie Administratora, chyba że taka automatyczna decyzja jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a Administratorem, lub jest wprost dozwolona przepisami prawa: albo opiera się o wyraźną zgodę odwołującej osoby,

5. Szczegółowe procedury wykonywania praw określonych w rozdziale III RODO określa Załącznik Nr 8 - „Prawa osoby, której dane dotyczą - procedury”.

**§7**

**Minimalizacja**

Administrator dba o minimalizację przetwarzania danych pod kątem: adekwatności danych do celów (ilości danych i zakresu przetwarzania), dostępu do danych, czasu przechowywania danych.

1. Minimalizacja zakresu:
    1) Administrator weryfikuje zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO. Administrator dokonuje na bieżąco przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania,
    2) Administrator przeprowadza weryfikację co do ilości i zakresu przetwarzania danych zgodnie z zasadą ochrony danych w fazie projektowania i zasadą domyślnej ochrony danych („Privacy by design" & „Privacy by default"). W tym celu Administrator już na etapie projektowania zmian analizuje i rekomenduje wdrożenie odpowiednich środków technicznych i organizacyjnych, tak aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności,
2. Minimalizacja dostępu:
    1) Administrator stosuje ograniczenia dostępu do danych osobowych: prawne (zobowiązania do poufności, zakresy upoważnień), fizyczne (strefy dostępu, zamykanie pomieszczeń) i logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe),
    2) W PCPR stosuje się kontrolę dostępu fizycznego. Dokonuje się aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających. Dokonuje się na bieżąco przeglądu i aktualizacji ustanowionych użytkowników systemów. Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w procedurach bezpieczeństwa fizycznego (Załącznik Nr 9 „Zasady korzystania z pomieszczeń i sprzętu PCPR oraz zasady gospodarki kluczami ") oraz ta instrukcja do systemu informatycznego .
3. Minimalizacja czasu:
    1) Administrator przetwarza dane osobowe do czasu osiągnięcia celu. Termin przetwarzania danych określony został na podstawie przepisów prawa lub wynikający z przeprowadzonej analizy ich przydatności i wykazany w Rejestrze,
    2) Dane, których zakres przydatności ulega ograniczeniu są archiwizowane oraz znajdują się na kopiach zapasowych systemu informatycznego. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych. Zasady zarządzania okresem przechowywania danych i weryfikacji dalszej przydatności wynikają z obowiązujących przepisów prawa w zakresie archiwizacji.

**§8**

**Bezpieczeństwo**

Administrator:

1. zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych w PCPR,
2. zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:

1) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii. Przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:
   a) zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania - wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych,
   b) kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają,
   c) przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia,
   d) ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym ustala przydatność i stosuje takie środki i podejście jak:
      - pseudonimizacja,
      - szyfrowanie danych osobowych,
      - inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności,
      - integralności, dostępności i odporności systemów i usług przetwarzania,
      - środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
   e) Wzór procedury analizy ryzyka określa Załącznik Nr 10,
2) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie oraz jest to obowiązkowe na podstawie przepisów prawa (art. 35 RODO). Dla wypełnienia obowiązku przeprowadzenia oceny skutków dla ochrony danych stosuje się metodykę oceny skutków zgodnie z Załącznikiem nr 11 (Wzór - Ocena skutków dla ochrony danych),
3) dostosowuje środki ochrony danych do ustalonego ryzyka,
4) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Prezesowi Urzędu Ochrony Danych Osobowych - zarządza incydentami,

3. Środki bezpieczeństwa. W PCPR stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych. Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa są bliżej opisane w procedurach przyjętych w PCPR dla tych obszarów,
4. Zestawienie środków organizacyjnych i technicznych zapewniających ochronę danych osobowych w zakresie poufności, integralności i rozliczalności:
   1) Ochrona danych osobowych polega na zabezpieczeniu informacji wprowadzonej, przetwarzanej, przesyłanej w systemie informatycznym oraz na nośnikach informacji przed nielegalnym ujawnieniem, kradzieżą oraz nieuprawnioną modyfikacją lub usunięciem,

2) W celu ochrony danych przechowywanych w systemach informatycznych należy wykorzystywać wchodzące w ich skład mechanizmy zarówno sprzętowe, jak i programowe oraz inne rozwiązania zwiększające bezpieczeństwo danych,
3) Dane osobowe mogą przetwarzać wyłącznie pracownicy upoważnieni do ich przetwarzania. Pracownicy upoważnieni do przetwarzania danych osobowych mają obowiązek zachować w tajemnicy dane, które przetwarzają oraz sposoby ich zabezpieczenia,
4) Wszystkie pomieszczenia, w których przetwarza się dane osobowe, są zamykane na klucz, w przypadku opuszczenia pomieszczenia przez ostatniego pracownika upoważnionego do przetwarzania danych osobowych - także w godzinach pracy,
5) Dane osobowe w formie papierowej są przechowywane po zakończeniu pracy w zamykanych na klucz szafach biurowych, a najlepiej w szafach metalowych. Klucze od szaf należy zabezpieczyć przed dostępem osób nieupoważnionych do przetwarzania danych osobowych. Zasady korzystania z pomieszczeń i sprzętu PCPR, zabezpieczenia ich po godzinach pracy oraz gospodarki kluczami określa Załącznik Nr 9 („Zasady korzystania z pomieszczeń i sprzętu PCPR, zabezpieczania ich po godzinach pracy oraz gospodarki kluczami.''),
6) Każdy pracownik zobowiązany jest do przechowywania na biurku tylko tych dokumentów, które są pracownikowi niezbędne w danym momencie pracy do wykonania bieżących zadań (tzw. polityka czystego biurka),
7) Na biurku nie mogą znajdować się napoje w pojemnikach grożących rozlaniem płynu,
8) Po zakończonej pracy na biurku może znajdować się jedynie telefon, komputer stacjonarny i przybory biurowe,
9) Próbne i zepsute wydruki papierowe powinny być niszczone w niszczarce dokumentów odpowiedniej klasy (np.:DIN4) w stopniu uniemożliwiającym ich odczytanie,
10) W przypadku żądania udostępniania danych osobowych pracownicy PCPR postępują zgodnie z przepisami RODO. Decyzję podejmuje Administrator na wniosek pracownika. Udostępnianie danych jest odnotowywane w systemach informatycznych i w formie papierowej,
11) Obszary przetwarzania danych osobowych są nadzorowane przez system monitoringu wizyjnego (w godzinach pracy) obsługiwany przez pracownika PCPR. Poza godzinami pracy PCPR funkcjonuje system zabezpieczeń fizycznych.
12) Procedury zarządzania uprawnieniami do systemów informatycznych reguluje Instrukcja zarządzania bezpieczeństwem systemów teleinformatycznych w PCPR (IZSI- załącznik nr 15).
13) Przy przetwarzaniu danych osobowych w systemach informatycznych należy stosować następujące zasady:
    a) kontrola dostępu do zbiorów danych osobowych,
    b) indywidualne identyfikatory użytkowników,
    c) uwierzytelnianie użytkowników systemu,
14) W celu zabezpieczenia danych osobowych przed ich utratą lub uszkodzeniem należy:
    a) dla wszystkich systemów stosować procedurę sporządzania kopii zapasowych, zgodnie z IZSI,
    b) systemy informatyczne wyposażyć w awaryjne zasilanie,
    c) stosować oprogramowanie antywirusowe,

d) kontrolować dostęp do systemów z publicznej sieci telekomunikacyjnej za pomocą zapory sieciowej, filtrów antyspamowych, oprogramowania antywirusowego, itp.,

15) stosować środki fizyczne chroniące urządzenia przed osobami nieupoważnionymi do dostępu do danych osobowych oraz zagrożeniami ze strony sił natury,
16) Użytkowników systemów obowiązuje polityka haseł opisana w IZSI,
17) Użytkownik systemu, który utracił hasło, zobowiązany skorzystać z serwisu odzyskiwania haseł (selfservice), ewentualnie skontaktować się z KSI,
18) W przypadku likwidacji, naprawy lub przekazania nośnika informacji, który zawiera dane osobowe, podmiotowi nieupoważnionemu do przetwarzania danych osobowych, należy zapewnić trwałe wymazanie informacji stanowiących dane osobowe, zgodnie z procedurami zawartymi w IZSI,
19) W przypadku korzystania z komputerów przenośnych, które zawierają dane osobowe należy zachować szczególną ostrożność podczas używania ich poza obszarem przetwarzania danych. Na użytkowanie przenośnych urządzeń komputerowych poza siedzibą PCPR wymagana jest zgoda Dyrektora. Szczegółowe zasady korzystania z komputerów przenośnych określa IZSI,
20) Ekrany komputerów, na których przetwarzane są dane osobowe, są chronione wygaszaczami zabezpieczonymi hasłem. Ekrany należy ustawić tak, aby dane osobowe były niewidoczne dla osób nieupoważnionych do ich przetwarzania lub stosować filtry anonimizacyjne,
21) Elektroniczne nośniki informacji zawierające dane osobowe muszą być zabezpieczone przed dostępem osób nieupoważnionych do ich przetwarzania. Sposób i miejsce ich przechowywania określa IZSI.

**§9**

**Zgłaszanie naruszeń ochrony danych osobowych**

1. Zgłaszanie naruszeń ochrony danych osobowych organowi nadzorczemu (instrukcja postępowania z incydentami). W procedurze opisano obowiązek zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu, terminy na dopełnienie tego obowiązku, minimalne wymogi co do treści zgłoszenia oraz sposób dokumentowania naruszeń,
   1) Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości,
   2) Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do natychmiastowego powiadamiania o wystąpieniu incydentu bezpieczeństwa, bezpośredniego przełożonego i Inspektora Ochrony Danych,
   3) Koordynator Systemu Informacji jest odpowiedzialny za uświadamianie pracowników o konieczności zgłaszania wykrytych sytuacji naruszenia bezpieczeństwa danych osobowych przetwarzanych w PCPR,
   4) Obsługę zgłoszonych przypadków związanych z naruszeniem bezpieczeństwa danych osobowych zapewniają pracownicy PCPR,

5) Punkt kontaktowy do zgłaszania przypadków związanych z naruszeniem bezpieczeństwa danych osobowych: w głównej siedzibie PCPR (Lubaczów ul. Piłsudskiego 80, w godzinach pracy 7.30 – 15.30., adres e-mail: justyna@ciechanowski.net.pl

2. Do typowych podatności mogących prowadzić do naruszenia bezpieczeństwa danych osobowych należą:
   1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
   2) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
   3) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek),
3. Pracownicy PCPR winni wzajemnie współpracować w celu minimalizacji podatności systemu ochrony danych osobowych,
4. Do typowych naruszeń bezpieczeństwa danych osobowych należą:
   1) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania, nieuprawnione modyfikowanie),
   2) przykładowe zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
   3) przykładowe zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych),
5. W przypadku wykrycia naruszenia bezpieczeństwa danych osobowych należy, o ile istnieje taka możliwość, niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, oraz uwzględnić w działaniu również ustalenie przyczyn lub sprawców. W szczególności należy:
   1) rozważyć wstrzymanie bieżącej pracy w celu zabezpieczenia miejsca zdarzenia (odłączyć urządzenie od sieci komputerowej, wylogować się z systemu, wyłączyć urządzenie),
   2) zaniechać, o ile to możliwe, dalszych działań, które wiążą się z zaistniałą sytuacją i mogą utrudnić jej udokumentowanie i późniejszą analizę,
   3) w zależności od okoliczności zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałej sytuacji (np. zasady BHP, ewakuacja z budynku, procedury ppoż.),
   4) poinformować pracowników PCPR wg zasad określonych w niniejszym dokumencie.
6. Zgłaszanie incydentu naruszenia bezpieczeństwa danych osobowych:
   1) Z uwagi na wymogi wynikające z RODO, w tym krótki okres na zgłoszenie incydentu naruszenia bezpieczeństwa danych osobowych (72 godziny od stwierdzenia/wykrycia naruszenia) informacje w tym zakresie muszą być przekazywane przez osoby lub podmiot przetwarzający dane, po zidentyfikowaniu zagrożenia, najpóźniej w ciągu 24 godz,
   2) Wykrycia naruszenia lub podejrzenie wystąpienia zdarzenia, które może mieć wpływ na bezpieczeństwo przetwarzanych danych należy zgłosić do punktu kontaktowego,
   3) Zgłoszenie musi zawierać: datę i czas zdarzenia, imię i nazwisko osoby zgłaszającej, miejsce wystąpienia incydentu naruszenia bezpieczeństwa danych osobowych oraz jego krótki opis (wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą oraz

kategorie i przybliżoną liczbę wpisów danych osobowych, opisywać możliwe konsekwencje naruszenia ochrony danych osobowych),

4) Zgłoszenie o naruszeniu przepisów o ochronie danych osobowych pochodzi najczęściej od osoby zatrudnionej przez PCPR przy przetwarzaniu danych osobowych jak i z informacji od podmiotu przetwarzającego,
5) Jeśli zgłoszenia dokonuje podmiot przetwarzający na podstawie Umowy powierzenia lub podmiot świadczący usługi serwisowe to zgłoszenie musi nastąpić w ciągu 24 godz,

7. Analiza przypadków naruszenia bezpieczeństwa danych osobowych:
   1) Każdy zgłoszony przypadek musi zostać poddany analizie, w zakresie ustalenia czy naruszenie bezpieczeństwa danych osobowych jest incydentem bezpieczeństwa (prowadzi do utraty, zniszczenia, ujawnienia itd.), a w szczególności czy naruszenie to skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych np. jeśli naruszenie może prowadzić do kradzieży lub fałszowania tożsamości, straty finansowej, naruszenia dobrego imienia czy też naruszenia tajemnic prawnie chronionych,
   2) W trakcie analizy należy brać pod uwagę następujące elementy:
      a) wdrożone zabezpieczenia i ich funkcjonowanie (potwierdzenie ich skuteczności),
      b) zapisy (logi systemowe/rejestry) systemu teleinformatycznego, jeśli zachodzi podejrzenie utraty poufności przetwarzanych danych (np kradzież danych z bazy),
      c) poprawność funkcjonowania systemu - bazy danych jeśli zachodzi podejrzenie utraty integralności przetwarzanych danych (np. uszkodzenie bazy danych),
      d) zapisy (logi systemowe/nagrania/rejestry) systemów zabezpieczeń wspomagających ochronę systemów teleinformatycznych oraz przetwarzanych danych, jeśli zachodzi podejrzenie nieautoryzowanego dostępu do danych,
   3) Analiza przeprowadzana jest przez pracownika PCPR we współpracy z IOD i KSI.
8. W zależności od charakteru naruszenia w czynnościach, o których mowa w ust. 6 mogą zostać zaangażowani:
   1) inni pracownicy PCPR,
   2) KSI (w szczególności jeśli naruszenie jest związane z funkcjonowaniem systemu informatycznego),
9. W wyniku analizy i stwierdzenia wystąpienia incydentu, ustalenia zakresu, przyczyny incydentu oraz jego ewentualnych skutków, IOD:
   1) działa na rzecz przywrócenia działania organizacji po wystąpieniu incydentu,
   2) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia,
   3) inicjuje ewentualne działania dyscyplinujące.
10. IOD wraz z KSI dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja naruszeń prowadzona jest według Załącznika Nr 12 - „Rejestr naruszeń ochrony danych osobowych”,
11. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych osobowych,
12. O wystąpieniu sytuacji naruszenia bezpieczeństwa danych osobowych przetwarzanych w PCPR jest informowany Administrator danych (Załącznik Nr 13 - Wzór Raportu o naruszeniu danych osobowych),

13. Zawiadomienie organu nadzorczego o sytuacji naruszenia bezpieczeństwa danych osobowych,
    1) Jeżeli przeprowadzona analiza, o której mowa w ust. 7 wskazuje na to że doszło do naruszenia bezpieczeństwa danych osobowych (incydent bezpieczeństwa), które może skutkować ryzykiem naruszenia praw i wolności osób z dużym prawdopodobieństwem, informacja o tym zdarzeniu jest kierowana do Prezesa Urzędu Ochrony Danych Osobowych,
    2) Zgłoszenia naruszenia bezpieczeństwa danych osobowych dokonywane jest w sposób określony przez organ nadzorczy nie później niż 72 godziny od stwierdzenia (wykrycia) zdarzenia,
    3) Jeżeli zgłoszenie naruszenia bezpieczeństwa danych osobowych dokonane zostanie po upływie 72 godzin od stwierdzenia (wykrycia) zdarzenia musi ono zwierać wyjaśnienie przyczyn opóźnienia,
    4) Zgłoszenia naruszenia bezpieczeństwa danych osobowych dokonuje IOD lub osoba działająca w jego zastępstwie. Art.33 ust.3 RODO określa minimalne informacje, które musi zawierać zgłoszenie,
14. Zawiadomienie osoby której dane dotyczą o sytuacji naruszenia bezpieczeństwa jej danych osobowych,
    1) Jeżeli przeprowadzona analiza, o której mowa w ust. 7 wskazuje, że doszło do naruszenia bezpieczeństwa danych osobowych, które może skutkować wysokim ryzykiem naruszenia praw i wolności osób, informacja o tym zdarzeniu jest kierowana bez zbędnej zwłoki do osób których dane dotyczą,
    2) W myśl przepisu art. 34 ust. 2 RODO zawiadomienie osoby, której dane dotyczą, powinno jasnym i prostym językiem opisywać charakter naruszenia ochrony danych osobowych oraz przynajmniej:
        a) zawierać imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
        b) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
        c) opisywać 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,
    3) Zawiadomienia o naruszeniu powinno zostać przekazane zainteresowanym osobom, biorąc pod uwagę dostępne kanały komunikacji z nimi oraz koszty wysyłki korespondencji np. z uwagi na liczbę osób objętych zawiadomieniem:
        a) na adres e-mail (jeśli znany),
        b) sms (jeśli znany nr telefonu),
        c) listownie (jeśli znany adres),
    4) Zawiadomienie w formie, o której mowa powyżej nie jest wymagane jeśli:
        a) w celu zabezpieczenia danych Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,

b) Administrator po stwierdzeniu naruszenia zastosował (następnie) środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
c) bezpośrednie zawiadomienie nie jest również wymagane jeśli powodowałoby to poniesienie niewspółmiernie dużych nakładów pracy i środków finansowych ze strony Administratora. W tym przypadku należy wydać publiczny komunikat (informacja na stronie PCPR- BIP i stronie promocyjnej, jednorazowe ogłoszenie w dzienniku o zasięgu regionalnym),

15. Usuwanie naruszenia bezpieczeństwa danych osobowych:
    1) Po wykryciu naruszenia bezpieczeństwa danych osobowych analizowane są okoliczności związane z jego wystąpieniem oraz ustalany jest sposób rozwiązania problemu oraz, jeśli to konieczne, zabezpieczenie materiału dowodowego,
    2) W usuwanie naruszenia bezpieczeństwa danych osobowych zaangażowani są pracownicy PCPR, którzy w ramach powierzonych obowiązków zapewniają i nadzorują funkcjonowanie systemu służącego do przetwarzania danych osobowych,
    3) W przypadku gdy problem może zostać rozwiązany samodzielnie przez pracowników PCPR, należy to wykonać bez zbędnej zwłoki,
    4) W przypadku konieczności wykonania działań przez podmiot zewnętrzny, pracownik zajmujący się rozwiązaniem problemu powinien, używając ustalonych metod, poinformować o zdarzeniu ten podmiot, oraz razem z jego przedstawicielem uczestniczyć w rozwiązywaniu problemu,
    5) Po przywróceniu prawidłowego stanu bezpieczeństwa danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyny naruszenia oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości,
    6) Jeżeli przyczyną naruszenia bezpieczeństwa danych osobowych:
        a) był błąd osoby przetwarzającej dane, w szczególności użytkownika systemu teleinformatycznego, można przeprowadzić dodatkowe szkolenie lub przesłać stosowną informację do wszystkich użytkowników systemu o sposobie postępowania przy przetwarzaniu danych osobowych oraz zapewnieniu ich bezpieczeństwa,
        b) było uaktywnienie złośliwego kodu, należy ustalić źródło jego pochodzenia oraz wykonać zabezpieczenia antywirusowe,
        c) było zaniedbanie lub umyślne działanie ze strony osoby zatrudnionej przy przetwarzaniu danych osobowych, należy powiadomić przełożonego i ewentualnie wyciągnąć konsekwencje służbowe,
        d) było włamanie lub uszkodzenie systemu zabezpieczeń w celu pozyskania danych osobowych, należy dokonać szczegółowej analizy wdrożonych środków zabezpieczających w celu zapewnienia skuteczniejszej ochrony danych osobowych,
        e) był zły stan urządzeń lub sposób działania oprogramowania, należy niezwłocznie przeprowadzić kontrolne czynności serwisowe,
16. Naruszenia bezpieczeństwa danych osobowych są omawiane na posiedzeniach Zespołu ds. Bezpieczeństwa Informacji.

**§ 10**

**Przetwarzający**

1. Administrator korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Wymogi dotyczące powierzenia określa art.28 RODO,
2. Przepisy RODO wskazują, że podmiot przetwarzający może wykazać, iż daje wystarczające gwarancje m in. poprzez stosowanie odpowiedniego zatwierdzonego przez Prezesa Urzędu Ochrony Danych Osobowych kodeksu postępowania albo poddał się procesowi certyfikacji i uzyskał certyfikat. Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora,
3. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian,
4. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie pisemnej umowy lub innego instrumentu prawnego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Umowa bądź porozumienie nie musi się ograniczać do kwestii powierzenia, może być ona elementem szerszej umowy (np umowy o współpracę, umowy serwisowej). Umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający:
    1) przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora (pisemna umowa powierzenia),
    2) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,
    3) podejmuje wszelkie środki wymagane na mocy art. 32 RODO,
    4) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w ust. 2 i 3,,
    5) 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 RODO,
    6) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32-36 RODO,
    7) przekazuje Administratorowi, w ciągu 24 godzin od wykrycia zdarzenia, informacje o naruszeniu ochrony powierzonych mu danych osobowych, w tym informacje niezbędne Administratorowi do zgłoszenia naruszenia ochrony danych organowi nadzorczemu, o którym mowa w art. 33 ust. 3 RODO. Zgłoszenie takie powinno odbywać się na adres: justyna@ciechanowski.net.pl
    8) zobowiązuje się do prowadzenia dokumentacji opisującej sposób przetwarzania danych, w tym rejestru kategorii czynności przetwarzania danych osobowych (wymóg art. 30 RODO) Przetwarzający udostępniania na żądanie Administratora prowadzony rejestr czynności przetwarzania danych przetwarzającego, z wyłączeniem informacji stanowiących tajemnicę handlową innych klientów Przetwarzającego,

9) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie,
10) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym paragrafie oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich,
11) jeżeli do wykonania w imieniu administratora konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nakłada - na mocy umowy lub innego aktu prawnego, te same obowiązki ochrony danych jakie zostały na niego nałożone umową z administratorem, o których to obowiązkach mowa w niniejszym ustępie, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom RODO,
12) jeżeli ten inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na pierwotnym podmiocie przetwarzającym,

**§ 11**

**Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych**

1. W przypadku wystąpienia przekazania danych osobowych do państw trzecich lub organizacji międzynarodowych Administrator zastosuje zasady opisane w Rozdziale V RODO,
2. W razie braku decyzji stwierdzającej odpowiedni stopień ochrony określonej w art. 45 ust 3 RODO lub braku odpowiednich zabezpieczeń określonych w art. 46 RODO, w tym wiążących reguł korporacyjnych, jednorazowe lub wielokrotne przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej nastąpi wyłącznie pod warunkiem, spełnienia wymagań określonych w art.49 RODO,
3. pracownicy są odpowiedzialni za monitorowanie i rejestrację wszystkich przypadków eksportu danych, czyli przekazywania danych poza Europejski Obszar Gospodarczy, który stanowią kraje członkowskie Unii Europejskiej oraz Islandia, Lichtenstein i Norwegia,
4. O każdym przypadku wystąpienia konieczności przekazania danych osobowych do państw trzecich lub organizacji międzynarodowych pracownik informuje IOD,
5. Aby uniknąć sytuacji nieautoryzowanego eksportu danych w szczególności w związku z wykorzystaniem publicznie dostępnych usług chmurowych w PCPR weryfikuje zachowania użytkowników oraz w miarę możliwości udostępnia zgodne z prawem ochrony danych rozwiązania równoważne,
6. Informacja o przekazaniu danych osobowych poza Europejski Obszar Gospodarczy zostanie zawarta w „ Rejestrze” oraz „Rejestrze kategorii czynności przetwarzania”

**§ 12**

**Ochrona danych w fazie projektowania i domyślna ochrona danych**

1. Ochrona danych w fazie projektowania procesów odnoszących się do danych osobowych uwzględnia:
   1) stan wiedzy technicznej,
   2) koszt wdrażania,
   3) charakter, zakres, kontekst i cele przetwarzania,
   4) ryzyko naruszenia praw lub wolności osób fizycznych,

   tak aby zaprojektować i wdrożyć odpowiednie środki techniczne i organizacyjne w celu nadania przetwarzaniu danych niezbędnych zabezpieczeń chroniących prawa osób, których dane dotyczą,

2. Domyślna ochrona danych gwarantuje aby przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia konkretnego celu przetwarzania. Dotyczyć to będzie ilości zbieranych danych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności.
3. Zasada uwzględniania ochrony danych w fazie projektowania oraz zasada domyślnej ochrony danych ma zastosowanie przy realizacji zamówień publicznych.

**§ 13**

**Szkolenia**

1. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi zostaje poddana przeszkoleniu i zapoznana z przepisami PODO oraz RODO,
2. Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania (Załącznik Nr 6 - Wzór Oświadczenie o poufności),
3. Szkolenie organizuje IOD,
4. Szkolenie wewnętrzne z zasad ochrony danych osobowych odbywa za zgodnie z Załącznikiem Nr 14 - „Wzór - Plan szkolenia z zakresu znajomości zasad ochrony danych osobowych”.

**§ 14**

**Audyty**

1. Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania,
2. Administrator jest odpowiedzialny za planowanie i przeprowadzanie audytów wewnętrznych z roczną częstotliwością,
3. Programy audytów będą opracowywane biorąc pod uwagę ważność procesów przetwarzania oraz audytowanych obszarów, jak też wyniki wcześniejszych audytów. W planie audytu określone zostaną kryteria audytu, jego cel, zakres i ewentualnie metody,

**§ 15**

**Punkt kontaktowy RODO**

1. W celu usprawnienia procesu obsługi spraw związanych z czynnościami przetwarzania danych osobowych w PCPR. Administrator organizuje „Punkt kontaktowy RODO".
2. Obsługę „Punktu kontaktowego RODO" zapewniają pracownicy PCPR,
3. „Punkt kontaktowy RODO" zlokalizowany jest w głównej siedzibie PCPR (Lubaczów ul. Piłsudskiego 8) i funkcjonuje w godzinach pracy 7.30 – 15.30.,
4. Do głównych zadań „Punktu kontaktowego RODO" należy:
   1) udzielanie ustnych i pisemnych informacji osobom, których dane dotyczą we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych w PCPR,
   2) koordynacja spraw związanych z załatwianiem wniosków i udzielanie informacji osobom, których dane są przetwarzane w PCPR w trybie art. 15- 20 RODO,
   3) przyjmowanie zgłoszeń o wystąpieniu naruszenia bezpieczeństwa danych osobowych przetwarzanych w PCPR

**§ 16**

**Udostępnianie danych osobowych**

RODO wyróżnia dwa rodzaje udostępniania danych:

1. udostępnianie innemu administratorowi - jeden administrator udostępnia dane drugiemu i każdy z nich wykorzystuje je do realizacji własnych celów,
2. współadministrowanie - opisane § 5 ust.1 lit.7.
   1) Udostępnianie danych innemu administratorowi następuje:
      a) za wyraźną zgodą osoby, której dane dotyczą,
      b) na podstawie przepisów prawa (np. udostępnienie danych policji, prokuraturze, sądom),
      c) innemu administratorowi, jeżeli przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora 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 (dochodzenie roszczeń, zapobieganie oszustwom, marketing bezpośredni),
   2) W przypadku żądania udostępniania danych osobowych decyzję podejmuje Administrator na wniosek pracownika. Udostępnianie danych jest odnotowywane w systemach informatycznych i w formie papierowej, co pozwala na pełną kontrolę kto, w jakim celu (przesłanka legalizująca), kiedy, jakie dane pozyskał z systemu oraz zapewnienie rozliczalności udostępnianych danych

**§ 17**

**Przeglądy i aktualizacje**

PODO podlega przeglądowi i aktualizacji w przypadku:

1. zmian w przepisach prawa wymagających aktualizacji PODO,
2. innych znaczących zmian dotyczących bezpieczeństwa przetwarzania danych osobowych,
3. w celu realizacji rekomendacji i zaleceń wynikających z przeprowadzonych kontroli i audytów.

**§ 18**

Traci moc Zarządzenie Nr 5/2015 Dyrektora Powiatowego Centrum Pomocy Rodzinie w Lubaczowie z dnia 24 marca 2015 r. w sprawie wprowadzenia Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Powiatowym Centrum Pomocy Rodzinie w Lubaczowie.

**§ 19**

Polityka wchodzi w życie z dniem podpisania z mocą obowiązującą od 15.05.2018 r.