CENTRUM MEDYCZNE im. BITWY WARSZAWSKIEJ 1920 r.	DOKUMENT nr 5	Wydanie: III
	POLITYKA BEZPIECZEŃSTWA INFORMACJI	Data wydania: 2023.05.10

ORYGINAŁ:	WŁASNOŚĆ: Pełnomocnik ds. ZSZ

Żadna część dokumentu nie może być zmieniona ani kopiowana bez zgody Pełnomocnika ds. Zintegrowanego Systemu Zarządzania. Dokument dostępny jest w wersji papierowej u Pełnomocnika ds. Zintegrowanego Systemu Zarządzania oraz w wersji elektronicznej w Intranecie.

Opracował/a:	Dokonał/a zmian:	Sprawdził/a:	Zatwierdził do stosowania:
Inspektor Ochrony Danych	**Inspektor Ochrony Danych**	**Pełnomocnik Dyrektora ds. Zintegrowanego Systemu Zarządzania**	**Dyrektor**
Podpis:	Podpis:	Pełnomocnik Dyrektora ds. Zintegrowanego Systemu Zarządzania	DYREKTOR Centrum Medyczne im. Bitwy Warszawskiej 1920 r.
Patryk Płachetko	**Ewa Kowalewicz**	Podpis:	Podpis:
Imię i nazwisko	*Imię i nazwisko*	**Jolanta Król**	**Krzysztof Jarząbek**
Data: 01.04.2020	Data: 08.05.2023	*Imię i nazwisko*	*Imię i nazwisko*
		Data: 09.05.2023	Data: 10.05.2023

DATA:	OPIS ZMIAN:
08.05.2023	• Zmiana w zakresie wstępu co do podstawy prawnej • Zmiana w zakresie stosowanych pojęć • Zmiana w zakresie podstawy prawnej analizy ryzyka • Zmiana w zakresie pkt 3.3 • Zmiany w zakresie zapisów dotyczących incydentów oraz naruszeń • Zmiany w zakresie zapisów dotyczących szkoleń oraz rejestru czynności przetwarzania • Zmiany w zakresie zapisów dotyczących wykazu zabezpieczeń • Zmiany w zakresie zapisów dotyczących rejestru żądań podmiotów danych

1. WSTĘP

Polityka bezpieczeństwa jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań 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) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.), zwanej RODO.

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z tym rozporządzeniem, a także usprawnienie i usystematyzowanie organizacji pracy Administratora.

2. DEFINICJE

Administrator (danych) - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych, w ramach niniejszego dokumentu jest to Centrum Medyczne im Bitwy Warszawskiej 1920 r w Radzyminie – SPZ ZOZ z siedzibą w Radzymin, ul. Konstytucji 3 Maja 17, 05-250 Radzymin.

RODO – rozporządzenie parlamentu europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 4 maja 2016 r.).

Dane osobowe - to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną przez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników specyficznych dla fizycznego, fizjologicznego, genetycznego, umysłowego, ekonomicznego, kulturowego lub społecznego. tożsamość tej osoby fizycznej.

Przetwarzanie danych osobowych to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych i obejmuje zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych.

Ograniczenie przetwarzania - polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.

Anonimizacja - zmiana danych osobowych, w wyniku której dane te tracą charakter danych osobowych.

Zgoda osoby, której dane dotyczą - oznacza dowolne, dowolnie określone, konkretne, świadome i jednoznaczne wskazanie osoby, której dane dotyczą, za pomocą oświadczenia lub wyraźnego działania potwierdzającego, wyrażającego zgodę na przetwarzanie danych osobowych z nim związanych. Zgoda musi być udokumentowana we właściwy sposób, aby ją udowodnić.

Ocena skutków w ochronie danych - to proces przeprowadzany przez Administratora, jeśli jest wymagany przez obowiązujące prawo i, jeśli to konieczne, z uczestnictwem inspektora ochrony danych, przed przetwarzaniem, w przypadku, gdy istnieje prawdopodobieństwo wysokiego ryzyka dla praw i wolności osób fizycznych jako rodzaju przetwarzania danych osobowych i zachodzi wraz z wykorzystaniem nowych technologii, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania. Proces ten musi ocenić wpływ planowanych operacji przetwarzania na ochronę danych osobowych.

Podmiotem danych jest każda osoba fizyczna, która jest przedmiotem przetwarzanych danych.

Odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

Podmiot przetwarzający (procesor) to osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu Administratora.

Inspektor Ochrony Danych (IOD) - to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi/podmiotowi przetwarzającemu/pracownikom w zakresie obowiązującego prawa o ochronie danych i tej polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.

Pseudonimizacja - oznacza przetwarzanie danych osobowych w taki sposób (np. przez zastępowanie nazw liczbami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. listy referencyjnej nazwisk i numerów), pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym w celu zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Szczególne kategorie danych osobowych - ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach zawodowych i obejmują przetwarzanie danych genetycznych, dane biometryczne w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia, dane dotyczące naturalnego życie seksualne osoby lub orientację seksualną. W zależności od obowiązującego prawa, specjalne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych i karnych oraz o sankcjach.

Profilowanie – jest dowolną forma zautomatyzowanego przetwarzania danych osobowych, która 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.

Naruszenie ochrony danych osobowych - jest to przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

PUODO – Prezes Urzędu Ochrony Danych Osobowych, organ państwowy powołany do spraw ochrony danych osobowych.

Podmiot Danych – osoba, której dane osobowe dotyczą.

3. OCENA SKUTKÓW (ANALIZA RYZYKA)

Ocena skutków jest formalną, określoną w art. 25 i art. 32 RODO procedurą przeprowadzenia analizy ryzyka za wykonanie której odpowiada Administrator. Jeżeli Administrator nie jest zobowiązany do przeprowadzenia oceny skutków, może mimo to stosować tę procedurę do przeprowadzenia analizy ryzyka na potrzeby wykazania rozliczalności spełnienia wymagań RODO.

W przypadku powołania Inspektora Ochrony Danych – ocena skutków musi być wykonana z jego współudziałem oraz po wyrażeniu przez niego opinii.

3.1. Opis operacji przetwarzania (INWENTARYZACJA AKTYWÓW)

W celu dokonania analizy ryzyka wymagane jest zidentyfikowanie danych osobowych, które należy zabezpieczyć.

3.2. Ocena niezbędności oraz proporcjonalności (zgodność z przepisami RODO)

W ramach przeprowadzenia oceny skutków (analizy ryzyka) Administrator zobowiązany jest do spełnienia wobec nich obowiązków prawnych. Należy przede wszystkim zapewnić, że :

1. dane te są legalnie przetwarzane (na podstawie art. 6, 9 RODO),
2. dane te są adekwatne w stosunku do celów przetwarzania,
3. dane te są przetwarzane przez określony czas – zasada ograniczonego czasu,
4. wobec tych osób wykonano tzw. obowiązek informacyjny (art. 12, 13 i 14 RODO) wraz ze wskazaniem ich praw (np. prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, odwołania zgody),
5. opracowano klauzule informacyjne dla powyższych osób,
6. istnieją umowy powierzenia z podmiotami przetwarzającymi (art. 28 RODO).

3.3. Analiza ryzyka

Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.
Analiza ryzyka powinna być dokonana na podstawie obecnej sytuacji w organizacji, z uwzględnieniem incydentów, które miały miejsce dotychczas, zidentyfikowanych procesów przetwarzania danych osobowych oraz raportu oceny ryzyka jeśli taki został stworzony.

3.4. Plan postępowania z ryzykiem

1. Wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne.
2. Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń
3. Upoważnienia.
4. Administrator odpowiada za nadawanie / anulowanie upoważnień do przetwarzania danych w zbiorach papierowych, systemach informatycznych.
5. Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie Administratora lub na podstawie przepisu prawa.

6. Upoważnienia nadawane są do zbiorów na wniosek przełożonych osób. Upoważnienia określają zakres operacji na danych, np. tworzenie, usuwanie, wgląd, przekazywanie.
7. Upoważnienia mogą być nadawane w formie poleceń, np. upoważnienia do przeprowadzenia kontroli, audytów, wykonania czynności służbowych, udokumentowanego polecenia Administratora w postaci umowy powierzenia
8. Administrator/Inspektor Ochrony Danych prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych.

4. Instrukcja postępowania z incydentami oraz naruszeniami

Zagrożeniem bezpieczeństwa informacji jest sytuacja, w której występuje zagrożenie zaistnienia incydentu. Przykładowy katalog zagrożeń:

1. nieprzestrzeganie Polityki przez osoby przetwarzające dane, np. niezamykanie pomieszczeń, szaf, biurek, brak stosowania zasad ochrony haseł,
2. niewłaściwe zabezpieczenie fizyczne dokumentów, urządzeń lub pomieszczeń,
3. niewłaściwe zabezpieczenie oprogramowania lub sprzętu IT przed wyciekiem, kradzieżą lub utratą danych osobowych.

Postępowanie Administratora danych osobowych lub osoby przez niego upoważnionej w przypadku stwierdzenia wystąpienia zagrożenia:

1. ustalenie zakresu i przyczyn zagrożenia oraz jego ewentualnych skutków,
2. w miarę możliwości przywrócenie stanu zgodnego z zasadami ochrony danych osobowych,
3. w razie konieczności zainicjowanie działań dyscyplinarnych,
4. zarekomendowanie działań zapobiegawczych w kierunku wyeliminowania podobnych zagrożeń w przyszłości,
5. udokumentowanie prowadzonego postępowania w rejestrze naruszeń bezpieczeństwa.

Incydentem jest sytuacja naruszenia bezpieczeństwa informacji ze względu na dostępność, integralność i poufność. Incydenty powinny być wykrywane, rejestrowane i monitorowane w celu zapobieżenia ich ponownemu wystąpieniu. Przykładowy katalog incydentów:

1. sytuacje losowe lub nieprzewidziane zdarzenia zewnętrzne (np. wybuch gazu, pożar, zalanie, katastrofa budowlana, napad, działanie terrorystyczne, niepożądane działanie ekipy remontowej itp.),
2. uszkodzenie sprzętu lub oprogramowania bezpośrednio wskazujące na umyślne działanie ukierunkowane na naruszenie ochrony danych, niewłaściwe działanie serwisu lub sam fakt pozostawienia serwisantów bez nadzoru,
3. pojawienie się alarmu z części systemu bezpośrednio odpowiadającej za ochronę zasobów,
4. niska jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inna nadzwyczajna i niepożądana modyfikacja w systemie,
5. wystąpienie naruszenia lub próba naruszenia integralności systemu,
6. wystąpienie niedopuszczalnej zmiany danych osobowych w systemie,
7. ujawnienie osobom trzecim danych osobowych lub objętych tajemnicą procedur przetwarzania danych lub innego strzeżonego elementu systemu zabezpieczeń,
8. wykazanie nieprzypadkowego odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych,
9. udostępnienie nieupoważnionym osobom dostępu do danych osobowych
10. skasowanie lub skopiowanie danych w niedozwolony sposób,

11. rażące naruszenie dyscypliny pracy w zakresie procedur bezpieczeństwa informacji (np. opuszczenie stanowiska bez wcześniejszego wylogowania lub odpowiedniego
12. zabezpieczenia stanowiska, pozostawienie danych osobowych na kserokopiarce, drukarce, nie zamknięcie pomieszczenia z komputerem, praca nad danymi w prywatnych celach, itp.)

Postępowanie Administratora/Inspektora Ochrony Danych lub właściwej osoby przez niego upoważnionej w przypadku stwierdzenia wystąpienia incydentu:

1. ustalenie czasu zdarzenia będącego incydentem oraz czasu wykrycia incydentu,
2. ustalenie zakresu incydentu,
3. określenie przyczyn, skutków oraz szacowanych zaistniałych szkód,
4. zabezpieczenie dowodów,
5. ustalenie osób odpowiedzialnych za naruszenie,
6. usunięcie skutków incydentu,
7. ograniczenie szkód wywołanych incydentem,
8. zainicjowanie działań dyscyplinarnych,
9. zarekomendowanie działań zapobiegawczych w kierunku wyeliminowania podobnych zagrożeń w przyszłości,
10. udokumentowanie prowadzonego postępowania w rejestrze naruszeń.

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych osoba stwierdzająca naruszenie zobowiązana jest:

a. powstrzymać się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów bądź innych dowodów naruszenia;
b. zabezpieczyć elementy infrastruktury IT lub dokumentację, przede wszystkim poprzez uniemożliwienie dostępu do nich osobom nieupoważnionym;
c. podjąć stosowne do zaistniałej sytuacji i niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych;
d. bezzwłocznie powiadomić o naruszeniu Administratora lub Inspektora Ochrony Danych i wykonywać jego polecenia.

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych Administrator, w imieniu, którego może działać Inspektor Ochrony Danych:

a. ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki;
b. ocenia zastałą sytuację;
c. wysłuchuje relacji osoby, która dokonała powiadomienia o incydencie;
d. podejmuje decyzje o toku dalszego postępowania;
e. dokumentuje prowadzone postępowanie;
f. dokonuje oceny ryzyka ewentualnego naruszenia;
g. wykonuje analizę incydentu, mającą na celu eliminację ich wystąpienia w przyszłości;
h. każdy incydent jest ewidencjonowany przez Administratora;
i. Administrator zgłasza naruszenie do PUODO zgodnie z art. 33 RODO.

W przypadku, gdy naruszenie ochrony danych osobowych jest wynikiem uchybienia obowiązującej dyscypliny pracy, Administrator wyjaśnia wszystkie okoliczności incydentu i podejmuje stosowne działania wobec osób, które dopuściły się wskazanego naruszenia.

Postępowanie w przypadku stwierdzenia wystąpienia zagrożenia do czasu przybycia Administratora lub upoważnionej przez niego osoby:

1. powstrzymanie się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów,
2. zabezpieczenie elementów systemu informatycznego lub kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osób nieupoważnionych,
3. podjęcie, stosownie do zaistniałej sytuacji, wszelkich niezbędnych działań celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.

5. SZKOLENIA

1. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi powinna być poddana przeszkoleniu i zapoznana z przepisami RODO. Jeśli przeprowadzenie szkolenia nie jest możliwe, przekazywane są stosowne materiały dydaktyczne z zakresu ochrony danych osobowych.
2. Za przeprowadzenie szkolenia odpowiada Administrator/Inspektor Ochrony Danych.
3. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych wskazane jest udokumentowanie odbycia tego szkolenia
4. Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania.

6. REJESTR CZYNNOŚCI PRZETWARZANIA

W związku z obowiązkiem prowadzenia Rejestru Czynności Przetwarzania Danych Osobowych wynikającym z art. 30 ust. 1 RODO, który spoczywa na Administratorze, dokument taki został przygotowany i wdrożony.

7. AUDYTY

Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania, przynajmniej raz na rok.

8. WYKAZ ZABEZPIECZEŃ

Środki Organizacyjne

1. Opracowano i wdrożono niniejszą politykę bezpieczeństwa.
2. Opracowano i wdrożono instrukcję zarządzania systemem informatycznym.
3. Powołano Inspektora Ochrony Danych.
4. Powołano Administratora Systemu Informatycznego.
5. Do przetwarzania danych dopuszczono wyłącznie osoby posiadające ważne upoważnienia nadane przez Administratora Danych.
6. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych.
7. Osoby zatrudnione przy przetwarzaniu danych zaznajomiono z przepisami dotyczącymi ochrony danych osobowych.
8. Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie ochrony danych osobowych lub umożliwiono zapoznanie się ze stosownymi materiałami dydaktycznymi z tego zakresu.
9. Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.
10. Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązano do zachowania ich w tajemnicy;

11. Monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
12. Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.
13. Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych.
14. Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych.
15. Stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami przetwarzającymi dane osobowe. Podmioty, którym powierzane są dane osobowe są weryfikowani pod kątem zapewnienia bezpieczeństwa powierzonych danych.
16. W organizacji prowadzi się politykę czystego biurka i ekranu.

Środki ochrony fizycznych danych

1. Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi).
2. Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności ogniowej >= 30 min.
3. Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności na włamanie - drzwi klasy C.
4. Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy.
5. Dostęp do pomieszczeń, w których przetwarzany jest zbiory danych osobowych objęte są systemem kontroli dostępu.
6. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych.
7. Zbiór danych osobowych w formie papierowej jest przechowywany w zamkniętej niemetalowej szafie.
8. Zbiór danych osobowych w formie papierowej jest przechowywany w zamkniętej metalowej szafie.
9. Zbiór danych osobowych w formie papierowej jest przechowywany w zamkniętym sejfie lub kasie pancernej.
10. Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej niemetalowej szafie.
11. Kopie zapasowe/archiwalne zbioru danych osobowych są przechowywane w zamkniętej metalowej szafie
12. Kopie zapasowe/archiwalne zbioru danych osobowych są przechowywane w zamkniętym sejfie lub kasie pancernej.
13. Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy znajdującej się w wyznaczonych miejscach w ciągu komunikacyjnym.
14. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej

1. Zastosowano urządzenia typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
2. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, jest zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
3. Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.
4. Zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł.
5. Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.
6. Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.
7. Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.
8. Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.
9. Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
10. Użyto system Firewall do ochrony dostępu do sieci komputerowej.
11. Użyto system IDS/IPS do ochrony dostępu do sieci komputerowej.

Środki ochrony w ramach narzędzi programowych i baz danych

1. Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.
2. Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.
3. Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
4. Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
5. Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.
6. Zastosowano kryptograficzne środki ochrony danych osobowych.
7. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
8. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

9. Rejestr żądań Podmiotów Danych

W związku z obowiązkiem realizacji praw osób, których dane dotyczą wynikających z art. 12-23 RODO oraz zasadą rozliczalności przed organem nadzorczym, który spoczywa na Administratorze, został stworzony i wdrożony rejestr żądań Podmiotów Danych.