Wydawca

Polityka Ochrony Danych Osobowych

Administrator Danych Osobowych:
Polska Izba Gospodarcza Czystości
ul. Bydgoskich Przemysłowców 6/106
85-862 Bydgoszcz

§ 1

Wstęp

Polityka Bezpieczeństwa Danych Osobowych, zwana dalej Polityką, została sporządzona w związku z wymaganiami Rozporządzenia Parlamentu Europejskiego i Rady (EU) 2016/679 z dnia 27 kwietnia 2016 roku 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 – dalej Rozporządzenie EU) oraz ustawy o ochronie danych osobowych.

Mając na uwadze prawo każdej osoby do ochrony i poszanowania prawa do prywatności, w szczególności prawa osób fizycznych powierzających do przetwarzania Administratorowi Danych swoje dane osobowe Polskiej Izbie Gospodarczej Czystości w Bydgoszczy, deklaruje podejmowanie wszelkich działań niezbędnych dla ochrony praw i usprawiedliwionych interesów jednostki, związanych z bezpieczeństwem danych osobowych. Jednocześnie gwarantuje stałe podnoszenie świadomości oraz kwalifikacji zatrudnionych w PIGC pracowników i osób wykonujących na jej rzecz zadania zlecone, a związane z przetwarzaniem danych osobowych.

Niniejszy dokument stanowi zbiór spójnych, precyzyjnych reguł i procedur, według których PIGC buduje, zarządza oraz udostępnia zasoby i systemy informacyjne i informatyczne. Ustanawia przewidziane do wykonania działania oraz sposób ustanowienia zasad i reguł postępowania koniecznych do zapewnienia właściwej ochrony przetwarzanych danych osobowych.

Polityka ustanawia zasady bezpieczeństwa przetwarzania danych osobowych, które powinny być przestrzegane i stosowane w PIGC przez wszystkie osoby przetwarzające dane osobowe, wraz z powołaniem na właściwe podstawy prawne. Polityka reguluje zasady organizacji pracy przy zbiorach danych osobowych przetwarzanych w systemie informatycznym oraz metodami tradycyjnymi. Opisano w niej również zagrożenia bezpieczeństwa przetwarzanych danych osobowych oraz sposoby reakcji na przypadki naruszeń bezpieczeństwa.

Niniejsza Polityka pełni także funkcję informacyjną i edukacyjną, poprzez zaprezentowanie obowiązków i odpowiedzialności osób związanych z przetwarzaniem danych osób związanych z przetwarzaniem danych osobowych.

PIGC stosuje adekwatne do sytuacji środki, aby zapewnić bezpieczeństwo informacji.

Dokumentacja zawiera także wskazania proceduralne dotyczące postępowań w przypadku naruszenia przepisów ochrony danych osobowych. Obejmuje ona wszystkich pracowników, jak i osoby

oraz podmioty współpracujące na podstawie umów cywilnoprawnych, mające jakikolwiek kontakt z danymi osobowymi objętymi ochroną w PIGC.

Uzupełnieniem niniejszej Polityki jest Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych (załącznik nr 1), ustanawiająca sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych.

§ 2

Podstawa prawna

Zasady przetwarzania danych osobowych regulują w szczególności:

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE;
2. Ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz.U. 2018 poz. 1000).

§ 3

Pojęcia użyte w Polityce Ochrony Danych Osobowych

Użyte w Polityce pojęcia oznaczają:

1. **Polityka** – oznacza niniejszą Politykę Ochrony Danych Osobowych.
2. **Ustawa** – Ustawę z dnia 10 maja 2018 roku o ochronie danych osobowych.
3. **RODO** – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 roku 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.
4. **Administrator Danych Osobowych** – PIGC z siedzibą w Bydgoszczy.
5. **Dane osobowe** – należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, przy czym możliwą do zidentyfikowania osobą fizyczną jest ta 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.

6. **Użytkownik** – osoba upoważniona do przetwarzania danych osobowych w PIGC.
7. **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 przesyłanie, rozpowszechnianie lub innego rodzaju udostępniania, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
8. **Podmiot przetwarzający** – oznacza fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.
9. **Zgoda** – oznacza zgodę osoby, której dane dotyczą tj. dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego potwierdzającego działania, przyzwala na przetwarzanie dotyczących jej danych osobowych.
10. **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.
11. **Pseudonimizacja** – oznacza przetworzenie danych osobowych w taki sposób, by nie było można ich 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. **Naruszenie ochrony danych osobowych** – oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
13. **Usuwanie danych osobowych** – zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
14. **Zabezpieczenie danych osobowych** – środki techniczne, organizacyjne i fizyczne wdrożone w celu zabezpieczenia danych osobowych oraz ich ochrony przed zniszczeniem, nieuprawnionym dostępem i modyfikacją, ujawnieniem lub pozyskaniem danych osobowych bądź ich utratą.
15. **Instrukcja** – Instrukcja Zarządzania Systemem Informatycznym.

16. **Pracownik** – osoba zatrudniona w PIGC na podstawie stosunku pracy lub innego stosunku prawnego.
17. **Integralność danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
18. **Kartoteka** – rozumie się przez to zewidencjonowany, usystematyzowany zbiór wykazów, skoroszytów, baz, wydruków komputerowych i innej dokumentacji gromadzonej w formie papierowej/elektronicznej, zawierającej dane osobowe.
19. **Integralność systemu** – rozumie się jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.
20. **Obszar przetwarzania** – należy przez to rozumieć pomieszczenia siedziby PIGC.
21. **Odbiorcy** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego czy jest stroną trzecią, przy czym organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są 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. **Pomieszczenia** – rozumie się przez to pomieszczenia lub części pomieszczeń tworzące obszar, w których przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego oraz gromadzone w kartotekach, wykazach, etc. również w sposób tradycyjny.
23. **Poufność danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym do tego osobom/podmiotom.
24. **Rozliczalność** – należy przez to rozumieć właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko danej (tej) osobie/ (danemu) temu podmiotowi danych (tych) informacji.
25. **Prezes Urzędu Ochrony Danych Osobowych** – należy przez to rozumieć krajowy, centralny organ do spraw ochrony danych osobowych, zwany dalej Prezesem Urzędu lub PUODO.
26. **Zagrożenie** – należy przez to rozumieć świadome lub nieświadome działanie, wskutek których doszło do utraty danych osobowych, kradzieży danych osobowych lub uszkodzenia nośników danych.

§ 4

Zakres stosowania

Przetwarzanie danych osobowych w PIGC odbywa się zgodnie z niniejszą procedurą zasad przetwarzania danych osobowych.

Za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Przy rozstrzyganiu czy określona informacja lub informacje stanowią dane osobowe, PIGC dokonuje zindywidualizowanej oceny przy uwzględnieniu konkretnych okoliczności oraz rodzaju środków czy metod potrzebnych w określonej sytuacji do identyfikacji osoby.

Natomiast osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Danymi osobowymi będą zarówno takie dane, które pozwalają na określenie tożsamości konkretnej osoby, jak i takie, które nie pozwalają na jej natychmiastową identyfikację, ale są, przy pewnym nakładzie kosztów, czasu i działań, wystarczające do jej ustalenia.

Zakresy ochrony danych osobowych określone w niniejszym dokumencie mają zastosowanie do każdej dokumentacji przetwarzanej w tradycyjnej formie papierowej, a zawierającej dane osobowe, oraz do systemów informatycznych, w których są przetwarzane dane osobowe, w szczególności do:

a) wszystkich istniejących, wdrażanych aktualnie lub w przyszłości (z zachowaniem zasad „privacy by design' – prywatności w fazie projektowania i „privacy by default" – prywatności w ustawieniach domyślnych) systemów informatycznym, w których przetwarzane są lub będą dane osobowe podlegające ochronie;
b) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane dane osobowe podlegające ochronie;
c) wszystkich pracowników oraz osób wykonujących czynności na rzecz PIGC, w ramach zawartych umów cywilnych i innych osób mających dostęp do informacji podlegających ochronie.

Do stosowania zasad określonych w niniejszej Polityce zobowiązani są wszyscy pracownicy oraz osoby wykonujące czynności na rzecz PIGC, w ramach zawartych umów cywilnych, jak również inne osoby mające dostęp do informacji podlegających ochronie.

§ 5

Podstawy przetwarzania danych osobowych

Przetwarzanie danych osobowych jest dopuszczalne wyłącznie na podstawie poniższych przesłanek:

1. kiedy osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
2. kiedy 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;
3. kiedy przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
4. kiedy przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej;
5. kiedy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
6. kiedy przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez osobę 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.

Przetwarzanie danych osobowych w PIGC nie może naruszać praw i wolności osób, których dane osobowe dotyczą, a w szczególności zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

W przypadku zbierania jakichkolwiek danych na potrzeby PIGC bezpośrednio od osoby, której dane dotyczą, Administrator Danych Osobowych jest zobowiązany do przekazania tej osobie następujących informacji:

a) swojej tożsamości i danych kontaktowych oraz, gdy ma to zastosowanie, tożsamości i danych kontaktowych swojego przedstawiciela;

b) gdy ma to zastosowanie – danych kontaktowych inspektora ochrony danych;
c) celów przetwarzania danych osobowych, oraz podstawy prawnej przetwarzania;
d) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) Rozporządzenia UE – prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią;
e) informacji o odbiorcach danych osobowych lub o kategoriach odbiorów, jeżeli istnieją;
f) gdy ma to zastosowanie – informacji o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony;
g) okresu, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteriów ustalania tego okresu;
h) informacji o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
i) jeżeli przetwarzanie odbywa się na podstawie zgody – informacji o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
j) informacji o prawie do wniesienia skargi do organu nadzorczego;
k) informacji, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualnie konsekwencje niepodania danych;
l) informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO oraz- przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Powyższe zasady nie mają zastosowania, w przypadkach gdy przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania lub jeżeli osoba, której dane dotyczą, posiada już te informacje.

W przypadku zbierania jakichkolwiek danych na potrzeby PIGC nie od osoby, której te dane dotyczą Administrator Danych Osobowych jest zobowiązany poinformować tę osobę dodatkowo o:

a) źródle pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł powszechnie dostępnych;
b) kategoriach odnośnych danych osobowych.

Powyższe zasady nie mają zastosowania, gdy:

a) przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą;
b) poinformowanie wymaga niewspółmiernie dużego wysiłku – w szczególności, gdy dane przetwarzane są w celach archiwizacyjnych, statystycznych bądź naukowych;
c) przekazanie informacji okazuje się niemożliwe;
d) utrwalenie lub ujawnienie danych jest wyraźnie nakazane prawem Unii lub prawem krajowym;
e) dotyczy to tajemnicy zawodowej wynikającej z prawa Unii lub prawa krajowego.

§ 6

Podstawowe zasady przetwarzania danych osobowych

PIGC jako Administrator Danych Osobowych dokłada najwyższej staranność, aby chronić interesy osób, których dane dotyczą, w szczególności dba o to, aby dane te były:

a) przetwarzane zgodnie z prawem;
b) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami;
c) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane – informacje wynikające z danych przetwarzanych przez administratora są zgodne z prawdą, kompletne oraz aktualne. Administrator Danych Osobowych przetwarza dane tylko w takim zakresie, w jakim jest to niezbędne do wypełnienia celu, w jakim dane są przez niego przetwarzane (zasada minimalizacji danych);
d) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celów przetwarzania;
e) Administrator Danych Osobowych stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzanie

z naruszeniem ustawy bądź rozporządzenia oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;

f) udostępniane wyłącznie w trybie określonym w rozporządzeniu lub ustawie, zgodnie z przypisami obowiązującego prawa.

Administrator Danych Osobowych dba o zachowanie bezpieczeństwa przetwarzanych danych osobowych oraz zapewnia poufność i integralność informacji, a także rozliczalność działań.

Poufność informacji oznacza, że informacje zawierające dane osobowe nie są udostępniane bądź ujawniane osobom nieupoważnionym, natomiast osoby nieuprawnione nie mają dostępu do danych osobowych.

Integralność informacji oznacza, że informacje są kompletne i niemożliwe jest ich zmienianie w jakikolwiek nieuprawniony sposób.

Rozliczalność działań oznacza, że wszystkie istotne czynności wykonane przy przetwarzaniu danych są zarejestrowane i jest możliwa identyfikacja osoby odpowiedzialnej na te czynności.

§ 7

Powierzenie przetwarzania danych osobowych

Przetwarzanie danych osobowych znajdujących się w PIGC może zostać powierzone podmiotowi zewnętrznemu.

Powierzenie przetwarzania danych osobowych odrębnym podmiotom odbywa się wyłącznie na podstawie pisemnej umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego 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.

Na podstawie umowy powierzenia podmiot przetwarzający ma obowiązek:

a) przetwarzać dane osobowe wyłącznie na udokumentowane polecenie administratora;

b) zapewnić by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;

c) zapewnić odpowiednie środki techniczne i organizacyjne w celu zabezpieczenia danych osobowych;

d) przestrzegać warunków korzystania z usług innego podmiotu przetwarzającego w przypadku dalszego powierzenia przetwarzania danych osobowych;
e) uwzględniając charakter przetwarzania, pomagać administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw jednostkowych określonych w RODO;
f) uwzględniając charakter przetwarzania oraz dostępne informacje, pomagać administratorowi wywiązać się z obowiązków nałożonych przez RODO;
g) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usunąć lub zwrócić mu wszelkie dane osobowe oraz usunąć wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;
h) udostępniać administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w RODO oraz umożliwić administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

Umowy powierzenia przed każdorazowym ich podpisaniem muszę być zaopiniowane przez Administratora Danych Osobowych.

Administrator Danych Osobowych prowadzi Ewidencję podmiotów, którym powierza dane osobowe. Ewidencja stanowi załącznik nr 2 do niniejszej Polityki.

Powierzenie danych osobowych do przetwarzania innemu podmiotowi nie jest tożsame z ich udostępnieniem tj. przekazaniem danych innemu podmiotowi (odbiorcy danych), który staje się ich administratorem. Powierzenie zaś polega na przetwarzaniu danych przez podmiot, który nie jest administratorem tych danych.

§ 8

Udostępnianie danych osobowych

Poprzez udostępnienie danych osobowych należy rozumieć wszelkie działania umożliwiające innym podmiotom, poza Administratorem Danych Osobowych, zapoznanie się z nimi.

a) Nie jest istotne czy udostępnianie danych osobowych ma charakter odpłatny czy nie, aby można było je uznać za udostępnienie;
b) Nie jest istotne, czy udostępnianie danych osobowych następuje w formie ustnej, pisemnej bądź za pomocą powszechnych środków przekazu lub poprzez sieć komputerową.

Dane osobowe przetwarzane zgodnie z RODO mogą być udostępniane jedynie na pisemny wniosek osoby, której dotyczą lub pisemny wniosek osoby upoważnionej przez tę osobę, jak również na wniosek podmiotu uprawnionego do ich otrzymania na mocy przepisów prawa, po pozytywnym zweryfikowaniu ustawowych przesłanek dopuszczalności takiego udostępnienia podmiotowi uprawnionemu.

Administrator Danych Osobowych prowadzi Ewidencję podmiotów, którym PIGC udostępnia dane osobowe. Ewidencja podmiotów stanowi załącznik nr 3 do niniejszej Polityki.

Ewidencja podmiotów zawiera informacje o udostępnieniu danych osobowych na rzecz wszystkich podmiotów, z wyłączeniem:

- osób upoważnionych do przetwarzania danych osobowych;
- osób, których dane dotyczą;
- organów państwowych lub samorządu terytorialnego, którym dane osobowe są udostępniane w związku z prowadzonym postępowaniem.

§ 9

Wykaz rejestru czynności przetwarzania

Przetwarzanie danych osobowych w PIGC dotyczy:

a) dopełnienia obowiązków pracodawcy określonych w przepisach prawa, związanych z zatrudnianiem pracowników, ubezpieczeniem, bezpieczeństwem i higieną pracy;
b) obsługi szkoleń;
c) walidacji i certyfikacji;
d) obsługi firm zrzeszonych w PIGC;

e) bazy wystawców targowych;
f) prenumeratorów Forum Czystości;
g) bazy partnerów PIGC.

Administrator Danych Osobowych prowadzi rejestr czynności przetwarzania danych osobowych, za które odpowiada. W rejestrze czynności przetwarzania zamieszcza się wszystkie następujące informacje:

a) nazwę oraz dane kontaktowe administratora;
b) cele przetwarzania;
c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
e) gdy ma to zastosowanie przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

Rejestr czynności przetwarzania stanowi załącznik nr 4 do niniejszej Polityki.

PIGC, w przypadku gdy jest podmiotem przetwarzającym zobowiązany jest do prowadzenia rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora. W rejestrze kategorii czynności przetwarzania zamieszcza się następujące informacje:

a) nazwę oraz dane kontaktowe podmiotu przetwarzającego oraz każdego administratora w imieniu którego działa podmiot przetwarzający;
b) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
c) gdy ma to zastosowanie – przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
d) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

Rejestr kategorii czynności przetwarzania stanowi załącznik nr 5 do niniejszej Polityki.

§ 10

Upoważnienie do przetwarzania danych osobowych

1. Do przetwarzania danych osobowych uprawnione są wyłącznie osoby upoważnione do przetwarzania danych osobowych.
2. W przedmiocie przyznawania upoważnień do przetwarzania danych osobowych uprawniony jest Administrator Danych Osobowych.
3. Upoważnienie do przetwarzania danych osobowych wymaga dla ważność formy pisemnej.
4. Wzór upoważnienia stanowi załącznik nr 6 do niniejszej Polityki.
5. Upoważnienie do przetwarzania danych osobowych następuje wyłącznie na podstawie indywidualnego upoważnienia nadanego zgodnie z przepisami prawa.
6. Nadanie upoważnienia do przetwarzania danych osobowych musi nastąpić przed rozpoczęciem przetwarzania danych osobowych przez osobę nieupoważnioną.
7. Administrator Danych Osobowych prowadzi Ewidencję osób upoważnionych do przetwarzania danych osobowych. Ewidencja osób upoważnionych do przetwarzania danych osobowych stanowi załącznik nr 7 do niniejszej Polityki.
8. Ewidencja osób upoważnionych zawiera następujące informacje:
   a) imię i nazwisko pracownika;
   b) identyfikator pracownika w systemie informatycznym służącym przetwarzaniu danych w PIGC;
   c) zakres przydzielonego upoważnienia;
   d) datę przyznania uprawnień;
   e) podpis Administratora Danych Osobowych potwierdzający przyznanie uprawnień;
   f) datę odebrania uprawnień (przy czym upoważnienie wygasa wraz z rozwiązaniem lub wygaśnięciem stosunku pracy);
   g) podpis Administratora Danych Osobowych potwierdzający odebranie uprawnień.
9. Każdy pracownik przed przystąpieniem do przetwarzania danych osobowych w PIGC jest zobowiązany do zapoznania się z przepisami dotyczącymi ochrony danych osobowych oraz z niniejszą Polityka Ochrony Danych Osobowych.
10. Pracownik przed przystąpieniem do przetwarzania danych osobowych potwierdza zapoznanie się z przepisami dotyczącymi ochrony danych osobowych oraz niniejszą Polityką poprzez złożenie podpisu na liście prowadzonej przez Administratora Danych Osobowych.

Oświadczenie pracownika o zapoznaniu się z przepisami w zakresie ochrony danych oraz z niniejszą Polityką stanowi załącznik nr 8 .

11. W przypadku konieczności nadania bądź zmiany uprawnień Administrator Danych Osobowych zobowiązany jest do przeszkolenia takiej osoby oraz do zaznajomienia jej z niniejszą Polityką.
12. Administrator Danych Osobowych jest odpowiedzialny za organizację i przeprowadzenie szkoleń lub zaznajomienie w innej formie osób upoważnionych z przepisami dotyczącymi ochrony danych osobowych.
13. Przetwarzanie danych osobowych przez osoby nieupoważnione przez Administratora Danych jest niedopuszczalne.
14. Osoby trzecie mogą przebywać na obszarze, w którym przetwarzane są dane osobowe jedynie w obecności Użytkownika, który posiada stosowne upoważnienie do przetwarzania.
15. Wszyscy pracownicy oraz osoba, o których mowa w pkt. 15 mają obowiązek zachowania tajemnicy o przetwarzanych danych osobowych oraz o stosowanych sposobach zabezpieczeń danych osobowych. Obowiązek zachowania poufności trwa mimo ustania zatrudnienia lub współpracy.

§ 11

Obowiązki podmiotowe w obszarze ochrony danych osobowych

Zadania w zakresie ochrony danych osobowych przetwarzanych w PIGC z siedzibą w Bydgoszczy realizują:

1. Prezes i Członkowie Zarządu PIGC;
2. Rada Programowa;
3. Komisja Rewizyjna;
4. Pracownicy PIGC;
5. Praktykanci;
6. Osoby fizyczne lub prawne świadczące usługi na rzecz PIGC.

I Obowiązki Administratora Danych Osobowych

a) organizacja bezpieczeństwa i ochrony danych osobowych w PIGC zgodnie z wymogami RODO oraz Ustawy o ochronie danych osobowych oraz innych przepisów regulujących zasady przetwarzania danych osobowych;
b) podział zadań i obowiązków związanych z organizacją ochrony danych osobowych;

c) ustalanie samodzielnie lub wspólnie z innymi celów i sposobów przetwarzania danych osobowych (z uwzględnieniem zmian zachodzących w przepisach prawa);
d) wydawanie i anulowanie upoważnień do przetwarzania danych osobowych w PIGC;
e) prowadzenie rejestru osób upoważnionych do przetwarzania danych osobowych zawierającego imię i nazwisko upoważnionego, datę nadania i ustania, zakres upoważnienia do przetwarzania danych osobowych, identyfikator w przypadku gdy upoważniony został zarejestrowany w systemie informatycznym, służącym do przetwarzania danych osobowych;
f) zawieranie umów związanych z przetwarzaniem, dostępem i pozbawianiem (usuwaniem) danych osobowych;
g) wykonywanie obowiązku informacyjnego wypełnianego przy zbieraniu danych osobowych, a także uzupełnianie, uaktualnianie, prostowanie danych osobowych, czasowe lub stałe ograniczenie przetwarzania danych osobowych lub ich usunięcie, gdy zażąda tego osoba, której dane są przetwarzane w PIGC;
h) podejmowanie właściwych działań w przypadku naruszenia lub podejrzenia naruszenia procedur przetwarzania danych osobowych, a także przepisów prawa w tym zakresie;
i) analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia ochrony danych osobowych i przygotowanie zaleceń i rekomendacji dotyczących eliminacji ryzyka ich ponownego wystąpienia;
j) zapewnienie podstaw prawnych do przetwarzania danych osobowych od chwili ich zebrania do chwili ich usunięcia;
k) wdrażanie odpowiednich środków technicznych i organizacyjnych w celu przetwarzania danych osobowych zgodnie z przepisami o ochronie danych osobowych (w szczególności RODO i Ustawy o ochronie danych osobowych);
l) wprowadzenie do stosowania procedur zapewniających prawidłowe przetwarzanie danych osobowych;
m) zgłaszanie organowi nadzorczemu, bez zbędnej zwłoki, nie później jednak niż w terminie 72h, stwierdzenia naruszenia ochrony danych osobowych, z wyłączeniem sytuacji małego prawdopodobieństwa naruszenia skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych;
n) zawiadamianie, bez zbędnej zwłoki osoby, której dane dotyczą o naruszeniu ochrony danych osobowych w przypadku możliwości wystąpienia wysokiego naruszenia jej praw lub wolności;
o) prowadzenie rejestru czynności przetwarzania w przypadku braku powołania IOD;

p) współpraca z organem nadzorczym w ramach wykonywanych zadań własnych;
q) w przypadku gdy dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, Administrator Danych Osobowych przez rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych (wzór oceny skutków przetwarzania stanowi załącznik nr 9 do niniejszej Polityki);
r) poddawanie przeglądom skuteczności Polityki Ochrony Danych Osobowych;
s) zapewnienie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez organizację i nadzorowanie przestrzegania zasad ochrony danych osobowych w systemach informatycznym, a także w zbiorach danych prowadzonych w formie papierowej i elektronicznej;
t) zapewnienie kontroli nad tym, jakie dane osobowe, przez kogo i kiedy zostały wprowadzone do zbioru.

II Obowiązki upoważnionych – pracowników oraz praktykantów upoważnionych do przetwarzania danych osobowych:

a) przetwarzanie danych osobowych wyłącznie w zakresie ustalonym indywidualnie przez Administratora Danych Osobowych w upoważnieniu i tyko w celu wykonywania nałożonych na niego obowiązków, przy czym rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych;
b) zachowanie w tajemnicy danych osobowych oraz przestrzeganie procedur wdrożonych w PIGC dotyczących ochrony danych osobowych i ich bezpieczne przetwarzanie, przy czym przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u Administratora Danych Osobowych, a także po ustaniu stosunku pracy, odwołania z pełnionej funkcji lub zakończenia współpracy;
c) znajomość niniejszej Polityki oraz przepisów powszechnie obowiązującego prawa w obszarze ochrony danych osobowych przetwarzanych przez PIGC;
d) zapoznawanie się na bieżąco z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami dokumentacji zawierającej zasady przetwarzania danych osobowych w PIGC;

e) stosowanie określonych przez Administratora Danych Osobowych procedur oraz wytycznych mających na celu zgodne z prawem, w tym zwłaszcza adekwatne przetwarzanie danych osobowych;

f) znajomość, zrozumienie i stosowanie w możliwie największym zakresie wszelkich dostępnych środków ochrony danych osobowych oraz uniemożliwienie osobom nieuprawnionym dostępu do swojej stacji roboczej;

g) zabezpieczanie danych osobowych przed ich udostępnianiem osobom nieupoważnionym;

h) Ochrona danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniekształceniem lub zniszczeniem;

i) informowanie przełożonego, o wszelkich podejrzeniach naruszania lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe.

§ 12

Ocena ryzyka i przeglądy

Zagrożenia zidentyfikowane w ramach przeprowadzonej analizy ryzyka nie wykazały wysokiego poziomu ryzyka.

1. Przegląd stanu ochrony przetwarzanych danych osobowych jest przeprowadzany co najmniej raz w roku.
2. Przegląd stanu ochrony przetwarzanych danych osobowych przeprowadza Administrator Danych Osobowych lub upoważniona w tym celu osoba.
3. Przeglądom poddawane są wszystkie obszary działalności i elementy infrastruktury PIGC, w których wymagane jest przestrzeganie zasad przetwarzania danych osobowych, w szczególności systemy informatyczne, zabezpieczenia fizyczne oraz organizacyjne.
4. Administrator Danych Osobowych lub osoba przez niego upoważniona przygotowuje plan przeglądu z uwzględnieniem jego zakresu oraz niezbędny, takich jak czas i ilość osób dokonujących czynności.
5. Z przeprowadzonego przeglądu sporządza się protokół.
6. Na podstawie raportu Administrator Danych Osobowych podejmuje działania zapobiegawcze.

§ 13

Zagrożenia bezpieczeństwa danych osobowych oraz incydenty

Na bezpieczeństwo procesu przetwarzania danych osobowych składają się:

- ✓ rozliczalność czyli możliwość przypisania działań osoby jednoznacznie i wyłącznie tej osobie;
- ✓ poufność czyli zapewnienie, że przetwarzane dane osobowe nie są udostępniane nieupoważnionym podmiotom;
- ✓ integralność czyli zapewnienie niemożliwości zmiany lub nieautoryzowanego zniszczenia danych osobowych.

1. Każdy pracownik, w przypadku stwierdzenia naruszenia ochrony danych osobowych lub ich zagrożenia, jest zobowiązany poinformować o tym fakcie swojego przełożonego lub właściwą upoważnioną osobę.
2. Osoba upoważniona lub przełożony są zobowiązani poinformować o fakcie, o którym mowa w pkt. 1 Administratora Danych Osobowych.

§ 14

Instrukcja postępowania w przypadku zagrożenia bezpieczeństwa danych osobowych

1. Zagrożenie bezpieczeństwa informacji to każda sytuacja, w której występuje zagrożenie zaistnienia incydentu.
2. Poprzez zagrożenie należy rozumieć:
   a) nieprzestrzeganie niniejszej Polityki przez osoby upoważnione do przetwarzania danych (niezamykanie pomieszczeń, szaf, biurek, brak stosowania haseł);
   b) niewłaściwe zabezpieczenie fizyczne dokumentów, urządzeń lub pomieszczeń;
   c) niewłaściwe zabezpieczenie oprogramowania lub sprzętu IT przed wyciekiem, kradzieżą lub utratą danych osobowych.
3. W przypadku stwierdzenia wystąpienia zagrożenia Administrator Danych Osobowych jest zobowiązany do:
   a) ustalenia zakresu i przyczyn zagrożenia oraz jego ewentualnych skutków;
   b) w miarę możliwości przywrócenia stanu zgodnego z zasadami ochrony danych osobowych;
   c) jeśli to konieczne, do podjęcia działań dyscyplinarnych;
   d) podjęcia działań zapobiegawczych w celu wyeliminowania podobnych zagrożeń w przyszłości;

e) udokumentowanie powyżej opisanego postępowania w Rejestrze naruszeń bezpieczeństwa, który stanowi załącznik nr 10 do niniejszej Polityki.

§ 15

Instrukcja postępowania w przypadku incydentów bezpieczeństwa danych osobowych

1. Incydentem jest każda sytuacja naruszenia bezpieczeństwa informacji ze względu na dostępność, integralność i poufność. Incydenty powinny być wykrywane, rejestrowane i monitorowane w celu zapobieżenia ich ponownemu wystąpieniu.
2. Poprzez incydenty należy rozumieć:
   a) losowe zdarzenia wewnętrzne (awaria komputera, serwera, twardego dysku, błąd użytkownika, informatyka, zgubienie danych);
   b) losowe zdarzenia zewnętrzne (klęski żywiołowe, zalanie, awaria zasilania, pożar, zalanie);
   c) Incydenty umyślne (wyciek informacji, ujawnienie danych nieupoważnionym osobom, świadome zniszczenie danych, działanie wirusów komputerowych, włamanie do pomieszczeń lub systemu informatycznego – wewnętrze i zewnętrzne).
3. W przypadku stwierdzenia wystąpienia incydentu Administrator Danych Osobowych jest zobowiązany do:
   a) ustalenia czasu zdarzenia będącego incydentem – powinien utrwalić w formie pisemnej wszelkie informacje i okoliczności związane z wystąpieniem incydentu, w szczególności powinien ustalić dokładny czas wystąpienia incydentu lub czas uzyskania informacji o wystąpieniu incydentu;
   b) ustalenia zakresu incydentu;
   c) określenia przyczyn oraz skutków, a także powinien oszacować powstałe szkody;
   d) zabezpieczenia dowodów naruszenia bezpieczeństwa danych osobowych;
   e) ustalenia osób odpowiedzialnych za naruszenie;
   f) usunięcia skutków naruszenia;
   g) podjęcie działań dyscyplinarnych wobec osób odpowiedzialnych za naruszenie;
   h) podjęcia działań zapobiegawczych w celu wyeliminowania podobnych zagrożeń w przyszłości;
   i) udokumentowania powyżej opisanego postępowania w Rejestrze naruszeń bezpieczeństwa, który stanowi załącznik nr 11 do niniejszej Polityki.

4. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego służącego przetwarzaniu danych osobowych Administrator Danych Osobowych jest zobowiązany do:
   a) wygenerowania i wydrukowania wszystkich dokumentów i raportów, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia;
   b) zidentyfikowania rodzaju zaistniałego zdarzenia, w szczególności określić szkody, metody dostępu osoby nieuprawnionej do przetwarzania danych osobowych w systemie informatycznym służącym do przetwarzania danych osobowych;
   c) podjęcia odpowiednich działań w celu powstrzymania lub ograniczenia dostępu osoby nieuprawnionej, zminimalizowania szkód;
   d) zabezpieczenia dowodów naruszenia ochrony danych osobowych poprzez:
      - fizyczne odłączenie urządzeń i segmentów sieci, które mogły umożliwić dostęp do danych osobie nieuprawnionej;
      - wylogowanie użytkownika podejrzanego o naruszenie ochrony danych osobowych;
      - zmianę hasła użytkownika, przez którego uzyskano nielegalny dostęp do danych osobowych e celu uniknięcia ponownej próby uzyskania takiego dostępu
      - analizę stanu systemu informatycznego służącego przetwarzaniu danych osobowych w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych;
      - przywrócenie normalnego działania systemu informatycznego służącego do przetwarzania danych osobowych.

§ 16

Procedury korzystania z urządzeń mobilnych w celach służbowych (smartfony, tablety, ipady)

1. Pracownik, który w zakresie powierzonych mu czynności służbowych korzysta z urządzenia mobilnego zobowiązany jest do stosowania w nim blokady dostępu w postaci hasła lub kody zabezpieczającego.
2. Dopuszczalne jest stosowanie zabezpieczenia w postaci odcisku linii papilarnych lub rysów twarzy, jednakże użycie takiego zabezpieczenia jest dobrowolne.

3. Użytkownik jest zobowiązany do chronienia urządzenia mobilnego przed kradzieżą, uszkodzeniem i dostępem osób postronnych, w szczególności do zachowania najwyższej ostrożności podczas transportu takiego urządzenia mobilnego.
4. Hasła dostępu do urządzeń mobilnych należy tworzyć zgodnie z obowiązującymi procedurami w PIGC.
5. W przypadku stosowania kodów zabezpieczających nie należy stosować prostych do złamania konfiguracji (np. 0000, 1111, 1234).
6. O ile jest to techniczne możliwe urządzenie mobilne powinno posiadać zainstalowaną aplikację antywirusową oraz zaporę sieciową.
7. Użytkownik urządzenia mobilnego zobowiązany jest do:
   a) systematycznego uaktualniania systemu operacyjnego na urządzeniu mobilnym;
   b) świadomego użytkowania Internetu w urządzeniu mobilnym tj. niekorzystania z nieznanych i niezabezpieczonych stron internetowych, niepobierania wiadomości i plików co do których pochodzenia i zawartości nie jest pewien, nieinstalowania aplikacji z nieautoryzowanych źródeł.
8. Zabrania się pracownikowi udostępniania lub umożliwiania korzystania z urządzenia mobilnego, na którym są przetwarzane dane osobowe, osobom postronnym.
9. W przypadku konieczności przekazania urządzenia mobilnego do serwisu, pracownik zobowiązany jest do usunięcia z pamięci urządzenia mobilnego wszelkich wiadomości e-mail, smsów, plików tymczasowych oraz historii przeglądarki internetowej, mogących zawierać informacje poufne lub dane osobowe podlegające ochronie. Informacje, które są niezbędne, przed usunięciem powinni zostać zapisane na innym nośniku danych.
10. Pracownik, który za pośrednictwem urządzenia mobilnego korzysta z bankowości elektronicznej, po wykonaniu czynności jest zobowiązany do wylogowania się z bankowości elektronicznej.
11. W przypadku niekorzystania z urządzenia mobilnego należy wyłączyć połączenia bezprzewodowe takie jak: WLAN, Bluetooth, GPS

§ 17
Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w których przetwarzane są dane osobowe

1. Polityka Bezpieczeństwa obowiązuje w PIGC w pomieszczeniach lub częściach pomieszczeń, w których przetwarzane są dane osobowe, a których wykaz został zamieszczony poniżej.
2. Polska Izba Gospodarcza Czystości mieści się pod adresem:
   ul. Bydgoskich Przemysłowców 6/106 85-862 Bydgoszcz.

LP	Lokalizacja – adres i nr budynku	Numer pomieszczenia /przeznaczenie/	Uwagi
1.			
2.			
3.			
4.			
5.			
6.			

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych

LP	Nazwa zbioru danych osobowych	System zastosowany do przetwarzania danych osobowych /nazwa systemu informatycznego/	Zakres danych osobowych w zbiorze danych/kategorie danych/	Komunikacja z innymi systemami	Przepływ danych
1.		Forma papierowa, poczta elektroniczna, dane w postaci plików PDF, plików word	Imię, nazwisko, adres, pesel, data urodzenia, miejsce urodzenia	Nie	Nie dotyczy
2.					
3.					
4.					
5.					

§ 18

Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Środki organizacyjne:

1. Do przetwarzania danych zostały dopuszczone wyłącznie osoby, którym nadano ważne upoważnienie.
2. Administrator Danych prowadzi ewidencję osób, którym nadano upoważnienia do przetwarzania danych.
3. Osoby zatrudnione przy przetwarzaniu danych osobowych zostały zapoznane z obowiązującą u Administratora Danych Polityką Ochrony Danych Osobowych oraz aktualnymi przepisami w zakresie ochrony danych osobowych.
4. Osoby zatrudnione przy przetwarzaniu danych osobowych zostały przeszkolone w zakresie zabezpieczeń systemu informatycznego.
5. Osoby zatrudnione przy przetwarzaniu danych osobowych zostały zobowiązane do zachowania poufności.
6. Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd w przetwarzane dane osobom postronnym.
7. Kopie zapasowe zbioru danych osobowych są przechowywane w oddzielnym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.
8. Przetwarzanie danych osobowych odbywa się w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych.
9. Osoby nie posiadające upoważnienia do przetwarzania danych osobowych, mogą przebywać w pomieszczeniach, gdzie są przetwarzane dane osobowe tylko w obecności osoby uprawnionej oraz w warunkach zapewniających bezpieczeństwo przetwarzania danych osobowych.
10. Powierzenie przetwarzania danych osobowych odbywa się wyłącznie na podstawie umowy zawartej w formie pisemnej pomiędzy Administratorem Danych a Podmiotem Przetwarzającym.
11. U Administratora Danych obowiązuje Polityka Czystego Biurka i Ekranu.

12. Każda z osób przetwarzająca dane osobowe ma obowiązek dbać o porządek na biurku i prawidłowe zabezpieczenie przechowywania dokumentów.

Środki fizyczne:

1. Wydzielono obszar przetwarzania danych osobowych.
2. Zbiory danych osobowych przechowywane są w pomieszczeniu zabezpieczonym drzwiami zwykłymi.
3. Pomieszczenia, w którym przetwarzane są dane osobowe zabezpieczone są drzwiami zamykanymi na klucz.
4. Klucze od szaf, w których są przechowywane dane osobowe znajdują się w specjalnej szafie zamykanej na klucz.
5. Dostęp do pomieszczeń, w których są przetwarzane dane osobowe posiadają wyłącznie osoby upoważnione do przetwarzania danych osobowych.
6. Dokumenty z aktami osobowymi są przechowywane w szafie zamkniętej na klucz.
7. Zbiory danych osobowych w formie papierowej przechowywane są w niemetalowej szafie zamkniętej na klucz.
8. Kopie zapasowe/archiwalne zbiorów danych osobowych przechowywane są innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.
9. Urządzenia, na których są przetwarzane dane osobowe umieszczone są w pomieszczeniach zamkniętych na klucz, do których mają dostęp tylko osoby uprawione.
10. Dokumenty zawierające dane osobowe po ustaniu celu przetwarzania są niszczone za pomocą niszczarki dokumentów lub oddawane specjalistycznej firmie zajmującej się utylizacją dokumentów. W przypadku utylizacji dokumentów przez firmę zawierana jest umowa o powierzenie przetwarzania danych osobowych.

Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej

1. Zbiory danych osobowych przetwarzane są na komputerach stacjonarnych oraz na komputerach przenośnych.
2. Komputery służące do przetwarzania danych nie są połączone z lokalną siecią komputerową.

3. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelniania przy użyciu identyfikatora użytkownika oraz hasła.
4. Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.
5. Wprowadzono wymóg okresowej zmiany haseł.
6. Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.
7. Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.
8. Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.
9. Zastosowano środki ochrony przed szkodliwym oprogramowaniem /np. program antywirusowy/.
10. Użyto system Firewall do ochrony dostępu do sieci komputerowej.
11. Narzędzia ochronne są regularnie aktualizowane, w tym oprogramowanie antywirusowe.
12. Na sprzęcie, na którym są przetwarzane dane osobowe, jest zainstalowane oryginalne oprogramowanie, regularnie aktualizowane.
13. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego.
14. Zastosowano mechanizmy kontroli dostępu do systemów informatycznych i ich zasobów; uprawnienia są różne dla różnych grup użytkowników.

Środki ochrony w ramach narzędzi programowanych i baz danych:

1. Zapewniono środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.
2. Wykorzystano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.
3. Dostęp do zbioru danych chroniony jest mechanizmem uwierzytelnienia za pomocą indywidualnego identyfikatora i hasła.
4. U Administratora Danych funkcjonują systemowe środki, które pozwalają na określenie odpowiednich praw dostępu do zbiorów danych osobowych dla poszczególnych osób uprawnionych.

5. Funkcjonuje system wymuszania okresowej zmiany haseł dostępu do systemów, w których są przetwarzane dane osobowe.
6. Administrator danych stosuje kryptograficzne środki ochrony danych osobowych.
7. Na stanowiskach komputerowych, na których dochodzi do przetwarzania danych osobowych ustawiono automatyczne wygaszacze ekranów.
8. W przypadku dłuższej nieaktywności pracy, następuje automatyczne wylogowanie z systemu/lub następuje automatyczna blokada systemu.

§ 19

Postanowienia końcowe

1. Polityka Ochrony Danych Osobowych wraz z załącznikami jest dokumentem obowiązującym w PIGC.
2. Wszystkie osoby upoważnione do przetwarzania danych osobowych są zobowiązane do przestrzegania postanowień zawartych w niniejszej Polityce.
3. Każda osoba, której obowiązki służbowe polegają na przetwarzaniu danych osobowych jest zobowiązana do zapoznania się z niniejszą Polityką.
4. Naruszenie zasad ochrony danych osobowych wynikających z niniejszej Polityki może być podstawą wszczęcia postępowania dyscyplinarnego.
5. Naruszenie zasad wynikających z niniejszej Polityki może być podstawą wszczęcia postępowania karnego wobec osoby, która dopuściła się naruszenia tychże zasad, a także może być podstawą dochodzenia roszczeń na drodze postępowania cywilnego.
6. W sprawach nieuregulowanych niniejszą Polityką znajdują zastosowanie przepisy RODO, Ustawy o Ochronie Danych Osobowych oraz przepisy powszechnie obowiązującego prawa regulującego kwestię ochrony danych osobowych.
7. Wszystkie załączniki stanowią integralną część niniejszej Polityki.