

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

.....
pieczęć firmowa

.....
podpis administratora danych osobowych

.....
data

Wstęp

Mając na uwadze konstytucyjne prawa każdego obywatela Rzeczypospolitej Polskiej:
KONSTYTUCJA RZECZYPOSPOLITEJ POLSKIEJ (ART. 47, 51):

(art. 47.)

Każdy ma prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.

(art. 51.)

1. Nikt nie może być obowiązany inaczej niż na podstawie **ustawy** do ujawniania informacji dotyczących jego osoby.
2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż **niezbędne** w demokratycznym państwie prawnym.
3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.
4. Każdy ma prawo do żądania **sprostowania** oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.
5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.

Zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. Z 2014 r., poz. 1182 ze zm.), art. 36 w/w ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, administrator danych osobowych zobowiązany jest do zapewnienia ochrony przetwarzanych danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Jakość zapewnianej ochrony powinna być odpowiednia do zagrożeń oraz kategorii danych nią objętych. Ponadto zgodnie z art. 38 ustawy administrator danych zobowiązany jest zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. Biorąc pod uwagę te konstytucyjne i ustawowe obowiązki wprowadzamy następujący zestaw procedur i rozwiązań, stanowiący Politykę bezpieczeństwa przetwarzania danych osobowych.

Rozdział 1 Postanowienia ogólne

§ 1. Ilekroć w Polityce jest mowa o:

- 1) **ustawie** – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2014 r., poz. 1182 ze zm.);
- 2) **danych osobowych** – **Art. 6.** ustawy: rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej; 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; informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań;

- 3) **zbiorniki danych** – **Art. 7.** ustawy: rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
- 4) **przetwarzaniu danych** – **Art. 7.** ustawy: rozumie się przez to jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
- 5) **systemie informatycznym** – **Art. 7.** ustawy: rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
- 6) **zabezpieczeniu danych w systemie informatycznym** – **Art. 7.** ustawy: rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
- 7) **usuwaniu danych** – **Art. 7.** ustawy: rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
- 8) **administratorze danych** – **Art. 7.** ustawy: rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, decydujące o celach i środkach przetwarzania danych osobowych;
- 9) **zgody osoby, której dane dotyczą** – **Art. 7.** ustawy: rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie;
- 10) **odbiorcy danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem osoby, której dane dotyczą, osoby upoważnionej do przetwarzania danych, przedstawiciela, o którym mowa w art. 31a ustawy, podmiotu, o którym mowa w art. 31 ustawy, organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;
- 11) **państwie trzecim** – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego (ang. *European Economic Area, EEA*) – strefa wolnego handlu i Wspólny Rynek.
- 12) **obszarze przetwarzania danych** – zgodnie z ustawą, przetwarzaniem danych osobowych nazywamy jakiegokolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych. W związku z powyższym, określanie obszaru pomieszczeń, w którym przetwarzane są dane osobowe, powinno obejmować zarówno te miejsca, w których wykonuje się operacje na nich (wpisuje, modyfikuje, kopiuje), jak również te, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową bądź komputerowymi nośnikami informacji z kopiami zapasowymi danych, stacje komputerowe, serwery i inne urządzenia komputerowe, jak np. macierze dyskowe, na których dane osobowe są przetwarzane na bieżąco). Zgodnie z treścią § 4 punkt 1 rozporządzenia miejsce przetwarzania danych osobowych powinno być określone

poprzez wskazanie budynków, pomieszczeń lub części pomieszczeń, w których przetwarza się dane osobowe.

- 13) **wykazie zbiorów** – należy przez to rozumieć wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
- 14) **opisie struktury zbiorów** – należy przez to rozumieć opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
- 15) **opis struktury zbiorów** – danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
- 16) **opisie przepływu danych** – należy przez to rozumieć opis sposobu przepływu danych pomiędzy poszczególnymi systemami informatycznymi;
- 17) **środkach technicznych i organizacyjnych** – należy przez to rozumieć środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

Rozdział 2

Administrator danych

§ 2. Administrator danych zobowiązany jest do podjęcia i wdrożenia następujących działań aby zapewnić pełną i całkowitą, niezbędną ochronę przetwarzanych zbiorów osobowych:

- 1) wdrożyć niniejszą Politykę bezpieczeństwa przetwarzania danych osobowych oraz Instrukcję zarządzania systemem informatycznym przetwarzającym dane osobowe;
- 2) upoważniać i cofać upoważnienia do przetwarzania danych osobowych osobom, które mają te dane przetwarzać, mają z nich korzystać na podstawie upoważnienia do przetwarzania danych osobowych w systemie informatycznym lub w zbiorze (załącznik nr 1);
- 3) prowadzić jasny i rzetelny wykaz osób upoważnionych do przetwarzania danych osobowych, dbać by osoby upoważnione kierowały się najwyższymi standardami ochrony prywatności, dbać by wykaz był aktualny i zawsze zgodny z prawdą (załącznik nr 2);
- 4) prowadzić wykaz obszarów przetwarzania danych osobowych (załącznik nr 3);
- 5) prowadzić wykaz zbiorów danych osobowych (załącznik nr 4);
- 6) prowadzić opis struktury zbiorów (załącznik nr 5);
- 7) prowadzić opis sposobu przepływu danych osobowych pomiędzy programami, środkami zarządzającymi tymi danymi (załącznik nr 6);

Rozdział 3

Środki techniczne i organizacyjne

§ 3. W celu ochrony danych spełniono wymogi, o których mowa w art. 36–39 ustawy:

- a) Administrator danych sam wykonuje czynności administratora bezpieczeństwa informacji;

- b) Do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych;
- c) Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych;
- d) Została opracowana i wdrożona Polityka bezpieczeństwa;
- e) Została opracowana i wdrożona Instrukcja zarządzania systemem informatycznym.

§ 4. W celu ochrony danych osobowych stosuje się następujące środki ochrony fizycznej danych osobowych:

- a) Zbiory danych osobowych w formie papierowej przechowywane są w zamkniętej metalowej szafie.
- b) Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi).
- c) Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

§ 5. W celu ochrony danych osobowych stosuje się następujące środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej:

- a) Komputer służący do przetwarzania danych osobowych nie jest połączony z lokalną siecią komputerową.
- b) Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
- c) Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.
- d) Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.
- e) Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.
- f) Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
- g) Użyto system Firewall do ochrony dostępu do sieci komputerowej.

§ 6. Środki ochrony w ramach narzędzi programowych i baz danych:

- a) Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.
- b) Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
- c) Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
- d) Zastosowano kryptograficzne środki ochrony danych osobowych.
- e) Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
- f) Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

§ 7. Środki organizacyjne:

- a) Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.
- b) Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.
- c) Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy.
- d) Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
- e) 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.

Rozdział 4 Postanowienia końcowe

§ 8. Polityka bezpieczeństwa jest bezwzględnie przestrzegana przez osoby upoważnione do przetwarzania danych osobowych, a nad jej przestrzeganiem czuwa administrator danych osobowych. Osoby upoważnione zostały w sposób prawidłowy i wyczerpujący poinformowane o prawach i obowiązkach na nich ciążyących ze szczególnym uwzględnieniem prywatności osób, których dane te dotyczą a która jest zagwarantowana przez Konstytucję, przepisy prawa i niniejszą Politykę Bezpieczeństwa.

§ 9. Administrator danych może w drodze umowy zawartej na piśmie tj. umowy o powierzeniu przetwarzania danych osobowych, powierzyć przetwarzanie danych innemu podmiotowi, który również zobowiązuje się do należytej i prawidłowej ochrony danych i prywatności osób, które zbiory te dotyczą. Podmiot ten może przetwarzać dane i informacje wyłącznie w zakresie niezbędnym dla realizacji swoich usług (na jakie zostały mu powierzone dane osobowe), przewidzianym w umowie oraz jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych o których mowa w art. 36–39 ustawy oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a ustawy. Odpowiedzialność podmiotu, o którym mowa wyżej jest taka sama jak administratora danych w zakresie powierzonych mu obowiązków. Za nieprzestrzeganie przepisów oraz polityki, odpowiedzialność ciąży na administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę o powierzeniu przetwarzania danych osobowych, za przetwarzanie danych niezgodnie z tą umową, w sposób wadliwy i niezapewniający należytej ochrony w myśl **Konstytucja Rzeczypospolitej Polskiej i ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych** oraz innych przepisów prawa.

§ 10. Polityka bezpieczeństwa wchodzi w życie z dniem zatwierdzenia jej przez administratora danych.

**UPOWAŻNIENIE ADMINISTRATORA DANYCH
do przetwarzania danych osobowych
w systemie informatycznym lub w zbiorze w wersji papierowej**

Z dniem upoważniam Panią/Pana
(*należy podać imię i nazwisko osoby upoważnionej*)

zamieszkałej/go w przy ul. nr PESEL.....

Zatrudnionej/zatrudnionego w
(nazwa jednostki organizacyjnej)

a) do obsługi systemu informatycznego w
(*należy podać nazwę administratora danych*)

w zakresie: zgodnego/ej z
przydzielonymi uprawnieniami dostępowymi do systemów informatycznych i w ramach tych
uprawnień; dostępu do danych osobowych.

(W) wglądu, (WP) wprowadzania, (MO) modyfikacji, (U) usuwania, (A) archiwizacji

b) do obsługi zbiorów danych w
(*należy podać nazwę administratora danych*)

w zakresie: zgodnego/ej z
przydzielonymi uprawnieniami dostępowymi do systemów informatycznych i w ramach tych
uprawnień; dostępu do danych osobowych.

(W) wglądu, (WP) wprowadzania, (MO) modyfikacji, (U) usuwania, (A) archiwizacji

Zobowiązuję Panią/Pana do bezwzględnego przestrzegania przepisów dotyczących ochrony danych osobowych, o których mowa w szczególności w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. Z 2014 r., poz. 1182 ze zm.). Do natychmiastowego informowania o przyczynach uniemożliwiających wypełnianie tego obowiązku oraz wprowadzonych i wdrożonych do stosowania przez Administratora Danych w „Polityce bezpieczeństwa” oraz w „Instrukcji zarządzania”.

Niniejsze upoważnienie traci moc najpóźniej z dniem odwołania, rozwiązania lub wygaśnięcia umowy o pracę, umowy zlecenia, umowy o dzieło lub innego stosunku prawnego.

.....

(miejsce i data)

.....

(pieczęć i podpis ABI)

OŚWIADCZENIE

Oświadczam, iż zostałam/em kompleksowo zapoznana/y z regulacjami przepisów prawnych dotyczącymi ochrony danych osobowych a w szczególności z:

- ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2014 r., poz. 1182 ze zm.) oraz wydanymi do tej ustawy aktami wykonawczymi regulującymi zakres ochrony danych osobowych;
- rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004r. Nr 100, poz. 1024)
- wprowadzonymi i wdrożonymi do stosowania przez administratora danych „Polityką bezpieczeństwa” oraz „Instrukcją zarządzania”.

Świadoma/y jestem że ciążą na mnie następujące obowiązki:

- niewykorzystywania danych osobowych Klientów w celach niezwiązanych z obowiązkami służbowymi, o ile nie są one zaaprobowane przez administratora danych osobowych w oparciu o obowiązujące przepisy prawa.
- zachowania w tajemnicy zastosowanych metod organizacyjnych, informatycznych i sprzętowych do ochrony danych osobowych, o ile nie są one jawne lub udostępnienia tych informacji nie żąda uprawniony do tego na podstawie przepisów prawa organ władzy państwowej,
- zachowania w ścisłej tajemnicy danych osobowych, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań powierzonych mi przez administratora danych oraz innych zobowiązań umownych lub obowiązków pracowniczych,
- korzystania ze sprzętu IT oraz oprogramowania wyłącznie w zakresie powierzonych uprawnień i w związku z wykonywaniem obowiązków pracowniczych lub zobowiązań umownych za zgodą i wiedzą administratora danych osobowych,
- wykorzystywania jedynie legalnego, oryginalnego, sprawnego oprogramowania zaakceptowanego i pochodzącego od administratora danych osobowych,
- pilnowania aby powierzony mi sprzęt i oprogramowanie było należycie używane i konserwowane, zgodnie z dokumentacją techniczną sprzętu oraz zgodnie z przepisami ochrony danych osobowych,
- w sytuacji korzystania z urządzeń przenośnych, dbania aby dane na nich udostępniane były należycie zabezpieczone zgodnie z dokumentacją ochrony danych osobowych,
- zachowania w tajemnicy danych osobowych Klientów nawet pomimo odwołania, rozwiązania lub wygaśnięcia umowy o pracę, umowy zlecenia, umowy o dzieło lub innego stosunku prawnego.

Powyższe zrozumiałam/em i zobowiązuję wypełniać wszystkie powierzone obowiązki z zakresu ochrony danych osobowych. Mam świadomość, iż postępowanie sprzeczne z powyższymi zobowiązaniami, zarówno celowe działania jak i zaniechania po mojej stronie mogą być uznane przez administratora danych osobowych za ciężkie naruszenie obowiązków pracowniczych lub zobowiązań umownych w rozumieniu przepisów prawa, a także rodzić odpowiedzialność karną wg. przepisów karnych w/w ustawy o ochronie danych osobowych i

prowadzić do powstania obowiązku odszkodowawczego za zaistniałą szkodę w myśl przepisów prawa.

podpis osoby upoważnionej

Wypełnia Administrator danego systemu:

Identyfikator użytkownika:

Data zarejestrowania w systemie:

Data wyrejestrowania użytkownika
(zablokowania dostępu) z systemu:

Podpis Administratora:

WYKAZ OSÓB/PACOWNIKÓW UPOWAŻNIONYCH W IMIENIU ADMINISTRATORA DO PRZETWARZANIA DANYCH OSOBOWYCH

	Imię i Nazwisko osoby upoważnionej	Przypisany numer Identyfikator w systemie informatycznym	Wersja papierowa upoważnienia	Data nadania upoważnienia	Data odebrania upoważnienia	Uwagi
1			Tak / Nie			
2			Tak / Nie			
3			Tak / Nie			
4			Tak / Nie			
5			Tak / Nie			

Dane aktualne na dzień:

Podpis w imieniu administratora danych:

**OBSZARY PRZETWARZANIA
DANYCH OSOBOWYCH KLIENTÓW**

	Nazwa obszaru	Zastosowane środki ochrony fizycznej danych	Zastosowane środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej	Zastosowane środki ochrony w ramach narzędzi programowych i baz danych	Zastosowane środki organizacyjne
1	Klienci	1,10,18	1,4,7,10,11,14,15	2,3,6,8,9,10	1,2,3,4,5
2					
3					
4					

Legenda:

Skróty oznaczenia środków ochrony fizycznej danych: 1 – drzwi zwykłe	Skróty oznaczenia środków sprzętowych infrastruktury informatycznej i telekomunikacyjnej: 1 – komputery nie połączone z lokalną	Skróty oznaczenia środków ochrony w ramach narzędzi programowych i baz danych: 1 – zastosowano rejestrację zmian w	Skróty oznaczenia środków organizacyjnych: 1 – osoby upoważnione zostały
--	---	--	--

<p>2 – drzwi o podwyższonej odporności ogniowej</p> <p>3 – drzwi o podwyższonej odporności na włamanie</p> <p>4 – okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej</p> <p>5 – system alarmowy przeciwwłamaniowy</p> <p>6 – system kontroli dostępu</p> <p>7 – system monitoringu z zastosowaniem kamer przemysłowych</p> <p>8 – służba ochrony</p> <p>9 – służba ochrony (całodobowo)</p> <p>10 – zamknięta niemetalowa szafa</p> <p>11 – zamknięta metalowa szafa</p> <p>12 – zamknięty sejf lub kasa pancerna</p> <p>13 – kopia zapasowa przechowywana w zamkniętej niemetalowej szafie</p> <p>14 – kopia zapasowa przechowywana w zamkniętej metalowej szafie</p> <p>15 – kopia zapasowa przechowywana w zamkniętym sejfie lub kasie pancernej</p> <p>16 – dane przechowywane w kancelarii tajnej</p> <p>17 – system przeciwpożarowy i/lub wolno stojąca gaśnica</p> <p>18 – niszczarki do dokumentów</p>	<p>sieci komputerową</p> <p>2 – zastosowano UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną</p> <p>3 – zastosowano hasło BIOS</p> <p>4 – zastosowano identyfikator użytkownika oraz hasło</p> <p>5 – zastosowano karty procesorowe oraz kod PIN lub token</p> <p>6 – zastosowano uwierzytelnienie (technologia biometryczna)</p> <p>7 – zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii</p> <p>8 – zastosowano systemową okresową zmianę haseł</p> <p>9 – zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych</p> <p>10 – zastosowano środki kryptograficznej ochrony danych w teletransmisji</p> <p>11 – zastosowano mechanizm uwierzytelnienia przy dostępie do środków teletransmisji</p> <p>12 – zastosowano procedurę oddzwonienia (callback) przy transmisji za pośrednictwem modemu</p> <p>13 – zastosowano macierz dyskową</p> <p>14 – zastosowano program antywirusowy</p> <p>15 – zastosowano system Firewall przy dostępie do sieci komputerowej</p>	<p>elementach zbioru danych</p> <p>2 – określono prawa dostępu do wskazanego zakresu danych</p> <p>3 – zastosowano identyfikator użytkownika oraz hasła</p> <p>4 – zastosowano karty procesorowe oraz kod PIN lub token</p> <p>5 – zastosowano technologię biometryczną</p> <p>6 – zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych</p> <p>7 – zastosowano okresową zmianę haseł dostępu</p> <p>8 – zastosowano kryptograficzne środki ochrony danych</p> <p>9 – zainstalowano wygaszacze ekranów</p> <p>10 – zastosowano automatyczną blokadę dostępu w przypadku dłuższej nieaktywności pracy użytkownika</p>	<p>zaznajomione z przepisami o ochronie danych</p> <p>2 – osoby upoważnione zostały przeszkolone z zabezpieczeń systemu informatycznego</p> <p>3 – osoby upoważnione zostały zobowiązane do zachowania danych w poufności</p> <p>4 – zastosowano politykę czystego ekranu</p> <p>5 – kopia zapasowa danych jest przechowywana w innym pomieszczeniu niż oryginał</p>
---	--	--	--

	16 – zastosowano system IDS/IPS		
--	---------------------------------	--	--

Dane aktualne na dzień:

Podpis w imieniu administratora danych:

WYKAZ ZBIORÓW DANYCH OSOBOWYCH

	Nazwa zbioru danych	Program przetwarzający dane osobowe	Rejestracja w GIODO	Data wpisu zbioru	Lokalizacja zbioru danych osobowych
1	<i>Baza danych klientów</i>		<i>RODO – brak obowiązku</i>		Siedziba firmy, magazyny, pomieszczenia przynależne.
2					
3					
4					

Dane aktualne na dzień:

Podpis w imieniu administratora danych:

OPIS STRUKTURY ZBIORÓW

Nazwa zbioru danych	Wersja papierowa	System informatyczny	Zawartość pól informacyjnych i powiązania pomiędzy nimi
<i>Baza danych klientów</i>	Nie	Tak	<i>dane adresowe klienta: [identyfikator klienta, imię, nazwisko, adres (kod pocztowy, miejscowość, ulica, nr domu/mieszkania), adres email], nr telefonu + zamówienia klienta: [identyfikator zamówienia, identyfikator klienta, identyfikator towaru, ilość towaru, wartość zamówienia, data zamówienia, data odbioru] +: [identyfikator towaru, nazwa towaru, nazwa producenta, data produkcji] + PESEL i data urodzenia klienta.</i>

Dane aktualne na dzień:

Podpis w imieniu administratora danych:

OPIS SPOSOBU PRZEPLYWU DANYCH

System (Moduł) A	System (Moduł) B	Kierunek przepływu danych osobowych	Sposób przesyłania danych osobowych
<i>Administrator</i>	<i>klient</i>	→	<i>Półautomatyczny</i>

Dane aktualne na dzień:

Podpis w imieniu administratora danych: