Spis treści

1. WPROWADZENIE I ZAKRES

W niniejszym dokumencie określono obowiązki Stron dotyczące ochrony danych w związku z procesem obsługi międzynarodowych i krajowych usług spedycyjnych, logistycznych, przewozowych, agencji celnych oraz innych związanych z obsługą obrotu towarowego (dalej: „Usługi"). W przypadku świadczenia przez Omida 7R Solutions Sp. z o.o. (dalej: Omida 7R) Usług na rzecz Klientów, Omida będzie pełniła rolę podmiotu przetwarzającego (dalej: Przetwarzający), a Klient będzie pełnił rolę Administratora. Omida 7R może występować również jako odrębny Administrator Danych, gdy powierza Usługę swoim Podwykonawcom, którzy będą pełnić rolę podmiotu przetwarzającego.

Dokument stosuje się do wszystkich czynności związanych z Usługą, w ramach których pracownicy Przetwarzającego lub Podwykonawcy zaangażowani przez Przetwarzającego przetwarzają dane osobowe (dalej: „Dane") Administratora.

W przypadku rozbieżności między bezwzględnie obowiązującymi postanowieniami Europejskich Standardowych Klauzul Umownych a postanowieniami niniejszej Polityki i dokumentów stanowiących jej część, postanowienia Europejskich Standardowych Klauzul Umownych będą nadrzędne. W przypadku innych rozbieżności między dokumentami, niniejsza Polityka będzie nadrzędna.

Niniejszą Politykę stosuje się do wszystkich czynności, w ramach których osoby zaangażowane w wykonywanie obowiązków na rzecz lub w imieniu Przetwarzającego mają styczność z danymi osobowymi Administratora.

Niniejsza Polityka ma zastosowanie na całym świecie w odniesieniu do wszystkich Usług świadczonych przez Omida 7R na rzecz Klienta.

Omida 7R zastrzega sobie prawo do aktualizacji niniejszej Polityki bez uzgadniania lub wcześniejszego informowania swoich Klientów.

2. DEFINICJE

#	Termin	Definicja
1	**Klient**	oznacza stronę Usługi zawartej z Omida 7R Solutions Sp. z o.o.
2	**RODO**	Rozporządzenie 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. Urz. UE L Nr 119 z 2016 r.
3	**Raporty z kontroli**	oznaczają aktualne zaświadczenia, raporty lub części raportów przygotowanych przez niezależne podmioty (np. biegłych rewidentów, audytorów wewnętrznych, inspektorów ochrony danych, dział bezpieczeństwa IT, audytorów ochrony danych, audytorów jakości) albo uznaną przez Administratora certyfikację na podstawie audytu bezpieczeństwa lub ochrony danych.
4	**Przetwarzanie danych**	oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub

		niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
5	**Dane**	oznaczają Dane osobowe określone w **załączniku nr 1**, które są przetwarzane przez Przetwarzającego w imieniu Administratora.
6	**Instrukcja**	oznacza instrukcję w formie pisemnej lub ustnej, udzieloną Przetwarzającemu przez Administratora, zobowiązującą Przetwarzającego do wykonania określonej czynności w odniesieniu do danych osobowych (takich jak m.in. pseudonimizacja, zablokowanie dostępu, usunięcie, udostępnienie danych).
7	**Dane osobowe**	oznaczają jakikolwiek element informacji osobistych lub rzeczowych na temat określonej lub możliwej do zidentyfikowania osoby fizycznej.
8	**Przetwarzanie w imieniu**	oznacza przetwarzanie danych osobowych w imieniu Administratora, w tym przechowywanie, modyfikowanie, przesyłanie, blokowanie dostępu i usunięcie danych osobowych przez Przetwarzającego.
11	**Techniczne i organizacyjne środki bezpieczeństwa**	oznaczają środki, których celem jest ochrona danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem lub dostępem, zwłaszcza jeśli przetwarzanie polega na przesyłaniu danych za pośrednictwem sieci, oraz ochrona danych osobowych przed wszelkimi innymi niezgodnymi z prawem formami przetwarzania. Powyższe środki obejmują m.in. pseudonimizację i szyfrowanie danych osobowych, zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, zdolność do przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu technicznego oraz regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

3. PRZEDMIOT, CEL, CZAS I ZAKRES PRZETWARZANIA DANYCH

Przedmiot i okres przetwarzania danych osobowych są zgodne z postanowieniami Usługi, zawartej pomiędzy Stronami.

Zakres, rodzaj i cel przetwarzania danych osobowych, jak również rodzaje Danych i podmiotów danych opisano szczegółowo w załączniku nr 1, który stanowi integralną część niniejszej Polityki. Przetwarzający będzie gromadził, przetwarzał i wykorzystywał Dane wyłącznie w celach określonych w załączniku nr 1.

4. PRAWO ADMINISTRATORA DO UDZIELANIA INSTRUKCJI

Przetwarzający będzie przetwarzał Dane wyłącznie zgodnie z postanowieniami Usługi oraz niniejszej Polityki, jak również zgodnie z Instrukcjami udzielonymi mu w tym zakresie przez Administratora, chyba że istnieje prawny obowiązek przetwarzania danych. W ramach Usług, Administrator zastrzega sobie prawo do podejmowania decyzji w zakresie charakteru, zakresu i metod przetwarzania danych, które to decyzje może wyrazić w poszczególnych Instrukcjach. Zmiany dotyczące celów i procedury wymagają zgody Stron

i udokumentowania. Przetwarzającemu wolno przekazywać informacje stronom trzecim lub podmiotom danych wyłącznie po uzyskaniu wcześniejszej pisemnej zgody Administratora.

Instrukcje Administratora będą mieć formę pisemną (co oznacza również formę wiadomości e-mail). W wyjątkowych przypadkach, Administrator może przekazywać Instrukcje w formie ustnej. Instrukcje w formie ustnej zostaną potwierdzone przez upoważnioną osobę po stronie Administratora na piśmie lub za pośrednictwem poczty elektronicznej (w formie tekstu).

Jeśli Przetwarzający uzna, że dana Instrukcja może skutkować naruszeniem obowiązujących przepisów prawa o ochronie danych osobowych, Przetwarzający niezwłocznie powiadomi o tym Administratora. W przypadku oczywistych naruszeń, Przetwarzający może wstrzymać wykonanie Instrukcji. Ponadto Przetwarzający ma prawo wstrzymać wykonanie Instrukcji do czasu potwierdzenia jej zgodności z prawem przez upoważnioną osobę po stronie Administratora lub do czasu zmiany takiej Instrukcji w formie pisemnej.

5. OBOWIĄZKI PRZETWARZAJĄCEGO

Przetwarzający wdroży techniczne i organizacyjne środki określone w **załączniku nr 2**, aby chronić Dane przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem, wykorzystaniem lub dostępem oraz przed wszelkimi innymi niezgodnymi z prawem formami przetwarzania.

Środki techniczne i organizacyjne będą rozwijane i aktualizowane stosownie do stanu wiedzy technicznej. W tym zakresie Przetwarzający może wdrożyć alternatywne stosowne środki za wcześniejszą pisemną zgodą Administratora. Poziom bezpieczeństwa zmienionych środków nie może być jednak niższy niż poziom zapewniony przez pierwotnie ustalone środki. Przetwarzający udokumentuje istotne zmiany i powiadomi o nich Administratora na piśmie lub pocztą elektroniczną. Przetwarzający będzie chronić infrastrukturę telekomunikacyjną przed złośliwym oprogramowaniem (program antywirusowy, zapora sieciowa). System operacyjny i inne oprogramowanie systemów IT będą niezwłocznie aktualizowane i poprawiane.

W przypadku wykonywania przez Przetwarzającego prac konserwacyjnych, które mogą prowadzić do znaczących odstępstw w zakresie przetwarzania danych osobowych Administratora względem głównej usługi (np. migracja na nowy system), Przetwarzający powiadomi wcześniej Administratora w odpowiedni sposób o planowanych pracach.

Przetwarzający będzie dokonywał regularnych przeglądów wewnętrznych procesów oraz środków technicznych i organizacyjnych, aby zapewnić zgodność przetwarzania danych w ramach swoich obowiązków z wymaganiami wynikającymi z prawa o ochronie danych osobowych, oraz zapewni ochronę praw podmiotów danych.

Przetwarzający udzieli Administratorowi wsparcia przy przygotowywaniu i aktualizowaniu wykazu czynności przetwarzania oraz przy ocenie niezbędnego zakresu ochrony danych i wcześniejszych konsultacjach. Na żądanie Administratora zostaną mu niezwłocznie udostępnione niezbędne informacje i dokumenty.

6. DALSZE POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH PRZEZ PRZETWARZAJĄCEGO

W rozumieniu niniejszej Polityki, Podwykonawcą jest podmiot, który świadczy usługi bezpośrednio związane z główną Usługą. Nie dotyczy to usług pomocniczych, takich jak usługi telekomunikacyjne, pocztowe i transportowe, konserwacja, obsługa użytkownika, rozporządzanie nośnikami danych oraz innymi zasobami sprzętowymi i oprogramowaniem. Jednak w ww. przypadkach Przetwarzający jest zobowiązany na mocy

umowy do zapewnienia ochrony i bezpieczeństwa danych oraz do zastosowania odpowiednich środków kontroli.

Jeśli w okresie obowiązywania Usługi zaistnieje konieczność zaangażowania Podwykonawcy, wymagana jest wcześniejsza pisemna zgoda Administratora. Dodatkowi/inny Podwykonawcy winni być w stanie spełnić takie same wymogi w zakresie ochrony danych, jakie uzgodniono z Przetwarzającym. Przetwarzający winien powiadomić Administratora na piśmie (lub za pośrednictwem poczty elektronicznej) przed udzieleniem zlecenia.

Obowiązki Przetwarzającego i Podwykonawcy muszą być wyraźnie rozgraniczone. W przypadku zaangażowania kilku Podwykonawców, powyższe dotyczy również obowiązków poszczególnych Podwykonawców.

Administrator ma prawo skierować zapytanie dotyczące treści istotnych obowiązków w zakresie ochrony danych i ich wykonania w ramach stosunków umownych między Przetwarzającym a Podwykonawcą przetwarzania, w razie potrzeby poprzez udostępnienie Administratorowi stosownych dokumentów umownych, oraz ma prawo uzyskać pisemną odpowiedź na takie zapytanie.

Jeśli jest to wymagane przez prawo, Przetwarzający zawrze dodatkowe umowy (m.in. zawierające Standardowe klauzule umowne zatwierdzone przez Komisję Europejską).

Ponadto Przetwarzający będzie chronił prawa Administratora określone w powyższych dokumentach również względem Podwykonawców, w tym zwłaszcza m.in. prawo Administratora do udzielania Instrukcji i przeprowadzenia kontroli.

7. PRAWO DO SPRAWOWANIA NADZORU I PRZEPROWADZENIA KONTROLI

Administrator ma prawo, lecz nie obowiązek, dwa razy w ciągu roku przeprowadzić kontrolę przestrzegania przez Przetwarzającego obowiązków w zakresie ochrony danych w dowolnej lokalizacji (np. kontrolę stosowania uzgodnionych środków technicznych i organizacyjnych) oraz bezpieczeństwa danych i bezpieczeństwa informatycznego. Ponadto Administrator ma prawo w każdej chwili przeprowadzić kontrolę z ważnej przyczyny (tzn. jeśli istnieje uzasadnione podejrzenie, że Przetwarzający naruszył swoje obowiązki dotyczące ochrony danych albo obowiązki dotyczące bezpieczeństwa danych i bezpieczeństwa informatycznego). Kontrola dotycząca ochrony danych może również być przeprowadzona przed przetwarzaniem danych oraz po zakończeniu przetwarzania. Na żądanie Administratora, Przetwarzający udzieli mu wsparcia przy sporządzaniu bieżących raportów z kontroli.

Administrator może zlecić wykonanie ww. kontroli pracownikom (w szczególności pracownikom odpowiedzialnym za ochronę danych i/lub bezpieczeństwo informacji) oraz zewnętrznym kontrolerom upoważnionym przez Administratora. Osoby, którymi Administrator posługuje się w celu przeprowadzenia kontroli (dalej „Audytorzy"), muszą zostać zobowiązani do zachowania poufności zgodnie z postanowieniami niniejszej Polityki. Aby chronić tajemnice handlowe Przetwarzającego oraz uniknąć podczas kontroli naruszenia obowiązku poufności Przetwarzającego wobec stron trzecich, Audytorzy zostaną zobowiązani w umowie przez Przetwarzającego do nieujawniania Administratorowi informacji, które Przetwarzający oznaczył jako poufne informacje stron trzecich. W odniesieniu do informacji oznaczonych jako informacje poufne stron trzecich, Audytorzy są zobowiązani udzielić odpowiedzi na ogólne pytania Administratora włącznie w celu zapewnienia przestrzegania umów zawartych przez Strony.

Administrator powiadomi Przetwarzającego ze stosownym wyprzedzeniem, ale nie później niż 14 dni wcześniej, o terminie i zakresie planowanej kontroli oraz wyznaczonych Audytorach. W przypadku kontroli

z ważnej przyczyny, powiadomienie o kontroli można przekazać również w terminie krótszym niż 14 dni przed datą planowanej kontroli.

Na potrzeby takiej kontroli, Audytorzy mogą skontrolować w zwykłych godzinach pracy Przetwarzającego lokalizacje, w których podlegające kontroli dane i dokumenty są przetwarzane lub przechowywane albo w których świadczone są określone usługi.

Przetwarzający umożliwi osobom przeprowadzającym kontrolę pełny dostęp do wyposażenia i systemów IT niezbędnych do przeprowadzenia kontroli (np. pomieszczenia centrów obliczeniowych, pomieszczenia z infrastrukturą informatyczną i nośnikami danych) oraz ujawni wszelkie informacje istotne dla kontroli w uporządkowanej, dostępnej i kompletnej formie. Przetwarzający zapewni Audytorom dostęp do odpowiednio wykwalifikowanych osób w celu wsparcia Audytorów przy przeprowadzaniu badania. Przetwarzający umożliwi Audytorom wykonania kopii danych i dokumentów istotnych dla kontroli oraz umożliwi im zabranie tych kopii ze sobą. Na prośbę Audytora, Przetwarzający prześle kopie takich dokumentów i danych do Audytorów.

W wyjątkowych przypadkach Przetwarzający może odmówić umożliwienia kontroli zapowiedzianej przez Administratora, jeśli przeprowadzenie kontroli wiązałoby się z nieuzasadnionym zakłóceniem działalności Przetwarzającego, przy czym Przetwarzający powiadomi Audytorów Administratora o innym terminie przeprowadzenia kontroli.

Administrator ponosi własne koszty przeprowadzenia kontroli. Administrator może zażądać od Przetwarzającego zwrotu takich kosztów, jeśli kontrola wykaże, iż Przetwarzający lub jego Podwykonawca w istotny sposób naruszył Politykę lub obowiązujące prawo.

8. ZGŁOSZENIE NARUSZENIA OCHRONY DANYCH PRZEZ PRZETWARZAJĄCEGO

Przetwarzający niezwłocznie powiadomi Administratora (w ciągu 36 godzin) o wszelkich naruszeniach lub podejrzeniach naruszenia przez Przetwarzającego, jego pracowników lub strony trzecie postanowień dotyczących przetwarzania Danych albo postanowień Usługi, Instrukcji i/lub postanowień niniejszej Polityki. W takim przypadku należy powiadomić koordynatora lub inspektora ochrony danych Administratora. W razie konieczności Administrator udostępni odpowiednie dokumenty na potrzeby zgłoszenia.

Strony udzielą sobie wzajemnie wsparcia przy usuwaniu wad lub nieprawidłowości w związku ze świadczeniem Usług. Jeśli podczas przetwarzania Danych wystąpią wady lub nieprawidłowości, Przetwarzający, ewentualnie wraz ze swoimi Podwykonawcami, niezwłocznie ustali przyczynę i podejmie wszelkie działania niezbędne do usunięcia wad i nieprawidłowości oraz zapobiegnięcia ich ponownemu wystąpieniu. Przetwarzający będzie niezwłocznie i na bieżąco informował Administratora o postępie podjętych działań aż do usunięcia problemu.

Zgodnie z obowiązującymi przepisami prawa, Strony mogą:

- być zobowiązane do przekazania właściwemu organowi nadzorczemu ds. ochrony danych wymaganych informacji zgodnie z pisemną instrukcją Administratora lub w zakresie wymaganym przez prawo;
- być zobowiązane do umożliwienia organowi nadzorczemu lub innym organom (m.in. organom ścigania) przeprowadzenia kontroli lub inspekcji w takim zakresie, w jakim kontrole mogą być wykonywane w obiektach Administratora lub Przetwarzającego.

W takich przypadkach:

- Strony udzielą sobie wzajemnie wsparcia w zakresie takich kontroli, o ile dotyczą one czynności przetwarzania danych przez Przetwarzającego na podstawie niniejszej Polityki; oraz
- Przetwarzający niezwłocznie powiadomi Administratora o kontrolach i środkach zastosowanych przez organy nadzorcze ds. ochrony danych albo inne organy w takim zakresie, w jakim takie powiadomienie jest dozwolone przez obowiązujące prawo.

9. PRAWA PODMIOTÓW DANYCH

Jeśli Administrator zostanie zobowiązany do udzielenia podmiotom danych informacji o przechowywaniu, wykorzystaniu lub innym przetwarzaniu danych osobowych podmiotów danych (określonych w art. 15-22 RODO), Przetwarzający udzieli takich informacji. Jeśli podmiot danych skontaktuje się z Przetwarzającym w związku z wykonaniem przysługujących mu na mocy prawa uprawnień, Przetwarzający niezwłocznie powiadomi Administratora i przekaże wniosek podmiotu danych.

Bez odpowiedniej Instrukcji Administratora, Przetwarzającemu nie wolno poprawiać, usuwać ani blokować dostępu do Danych.

10. ZASADY ZACHOWANIA POUFNOŚCI DANYCH

Przetwarzający jest zobowiązany chronić poufność danych zgodnie z obowiązującymi przepisami prawa o ochronie danych.

Przetwarzającemu wolno powierzać przetwarzanie i wykorzystanie Danych wyłącznie pracownikom, którzy zostali zobowiązani do zachowania poufności danych. W szczególności Przetwarzający zapewni staranny dobór personelu i zobowiąże wszystkie osoby, którym powierzono wykonanie niniejszej Polityki, do przestrzegania przepisów prawa dotyczących ochrony danych. Na żądanie Administratora, Przetwarzający przedstawi odpowiedni dowód przestrzegania powyższych obowiązków.

11. OBOWIĄZEK ZWROTU I USUNIĘCIA DANYCH

Przetwarzający jest zobowiązany przekazać Administratorowi wszelkie Dane, oryginalne nośniki danych (jeśli dotyczy) lub dokumenty, które zostały mu przekazane przez Administratora w celu świadczenia Usług, niezwłocznie po zakończeniu wykonywania obowiązków określonych w Usłudze (nie później niż w terminie 30 dni). Powyższy obowiązek dotyczy również dodatkowych dokumentów będących w posiadaniu Przetwarzającego podczas świadczenia Usług, w tym m.in. materiałów testowych (jeśli dotyczy).

Ponadto Przetwarzający jest zobowiązany zniszczyć dane osobowe w sposób określony w Usłudze lub zgodnie z przepisami dotyczącymi ochrony danych.

Powyższe postanowienia nie mają wpływu na ustawowy obowiązek Przetwarzającego dotyczący obowiązku przechowywania danych.

12. ODPOWIEDZIALNOŚĆ

Administrator i Przetwarzający ponoszą solidarną odpowiedzialność z tytułu roszczeń odszkodowawczych osób na skutek nieprawidłowego przetwarzania danych w ramach stosunku umownego.

W przypadku przetwarzania danych takiej osoby, na Przetwarzającym spoczywa ciężar udowodnienia, że szkoda nie została spowodowana z przyczyn leżących po jego stronie. W przypadku braku takiego dowodu, Przetwarzający, na pierwsze żądanie, zwolni Administratora ze wszelkich roszczeń dochodzonych wobec Administratora w związku z powierzonym przetwarzaniem danych.

Przetwarzający ponosi odpowiedzialność wobec Administratora za szkody powstałe z winy Przetwarzającego, jego pracowników lub Podwykonawców zaangażowanych przez Przetwarzającego w związku ze świadczeniem zleconych usług.

Powyższe nie dotyczy, jeśli szkoda powstała na skutek prawidłowego wykonania zleconej usługi lub instrukcji udzielonej przez Administratora.

13. POSTANOWIENIA KOŃCOWE

Z tytułu usług świadczonych na podstawie niniejszej Polityki nie przysługuje osobne wynagrodzenie. Pełne wynagrodzenie za te usługi określono w Usłudze.

Załącznik nr 1 – Dane, cele, podmioty danych

Przetwarzający przetwarza następujące Dane:

1. Rodzaj danych:

- imię i nazwisko;
- adres zamieszkania;
- adres prowadzonej działalności gospodarczej;
- numer telefonu;
- e-mail;
- narodowość;
- numer PESEL;
- numer dowodu osobistego;
- numer NIP;
- numer paszportu;
- numer konta bankowego;
- nazwa stanowiska;
- dane lokalizacyjne.

2. Cele: Dane są przetwarzane i wykorzystywane wyłącznie w celach opisanych w Usłudze.

3. Podmioty danych: Klienci oraz ich pracownicy.

Załącznik nr 2 – Środki techniczne i organizacyjne

Środki techniczne i organizacyjne, do których wdrożenia zobowiązany jest Przetwarzający zgodnie z niniejszą Polityką, powinny uwzględniać aktualny stan wiedzy technicznej, koszty wdrożenia jak również charakter, zakres, okoliczności i cele przetwarzania oraz prawdopodobieństwo i stopień zagrożenia praw i wolności osób. Do środków technicznych i organizacyjnych, do których wdrożenia zobowiązany jest Przetwarzający zgodnie z niniejszą Polityką, należą w szczególności:

1. Analiza ryzyka

Przetwarzający przeanalizował ryzyka związane z konkretnym przetwarzaniem, zwłaszcza ryzyka związane z usunięciem, naruszeniem, manipulacją i/lub nieuprawnionym dostępem i/lub przesyłaniem.

2. Ocena ryzyka

Należy ocenić ryzyka związane z zamierzonym przetwarzaniem (prawdopodobieństwo, stopień, podatności, aspekty, konsekwencje prawne itd.). Analizę i ocenę należy udokumentować, np. w ramach koncepcji ochrony danych oraz bezpieczeństwa informacji/bezpieczeństwa informatycznego.

3. Środki techniczne i organizacyjne

Do środków technicznych i organizacyjnych, do których wdrożenia zobowiązany jest Przetwarzający zgodnie z niniejszą Polityką, należą w szczególności:

SRODKI TECHNICZNE I ORGANIZACYJNE		
Poufność	Kontrola wstępu [pomieszczenia i budynki]	Wstęp do pomieszczeń biurowych tylko dla osób upoważnionych lub w ich towarzystwie
		Zabezpieczanie drzwi (elektryczne otwieranie drzwi, zamki bezpieczeństwa, wejście na kartę)
		W recepcji w godzinach odwiedzin zawsze jest pracownik
		Strefy bezpieczeństwa: serwery urządzeń przetwarzających dane znajdują się w osobnych pomieszczeniach, oddzielonych od zwykłych pomieszczeń biurowych i posiadają osobny system ochrony wstępu
		Służby ochrony poza godzinami odwiedzin
		Monitoring wideo przy wejściach do budynku
		System alarmowy
	Kontrola dostępu [systemy informatyczne i aplikacje]	Uwierzytelnianie za pomocą nazwy użytkownika i hasła
		Wymagania w zakresie złożoności haseł, blokady stanowisk pracy, użytkownicy mogą chronić sesję za pomocą wygaszacza ekranu z hasłem
		Indywidualny i powiązany z osobą login użytkownika przy logowaniu w sieci przedsiębiorstwa
		Stosowanie zapór sieciowych
		Stosowanie rozwiązań Endpoint Protection [rozszerzonego oprogramowania antywirusowego]
		Stosowanie technologii VPN
		Centralna kontrola uprawnień [AD]

	Kontrola dostępu [do danych i informacji]	Fizyczne usuwanie danych z nośników danych przed ich utylizacją
		Korzystanie z certyfikowanych usługodawców w zakresie niszczenia akt i danych
		Centralna koncepcja uprawnień [przyznawanie uprawnień według zasady minimalizacji, przyznawanie i korzystanie z uprawnień administratora ograniczone do niezbędnego minimum, weryfikacja uprawnień dostępu, oddzielne przyznawanie uprawnień (organizacyjnie) i ich nadawanie (techniczne)]
		Zróżnicowane i związane z zadaniami uprawnienia, profile i role
		Zarządzanie uprawnieniami użytkowników przez administratorów systemu
		Wytyczne dotyczące haseł definiujące także ich długość i zmianę
	Rozdzielność	Techniczne rozdzielenie systemów produkcyjnych i testowych
		Koncepcja uprawnień w celu rozdzielenia systemów produkcyjnych i projektowych
		Oddzielne bazy danych
		Oddzielne struktury folderów i katalogów
		Oddzielne miejsca przechowywania danych z koncepcją uprawnień i ról w ramach przetwarzania danych na zlecenie
Integralność	Kontrola przekazywania	Zabezpieczona sieć WLAN
		Tunelowane połączenie danych za pomocą technologii VPN
		Komunikacja pocztą elektroniczną poprzez szyfrowanie
		Staranny wybór usługodawców [np. w zakresie niszczenia akt i nośników danych]
Dostępność i odporność	Kontrola dostępności	System sygnalizacji pożarowej
		Koncepcja kopii zapasowych [codziennie, co tydzień, co miesiąc]
		Koncepcja ochrony antywirusowej / zapora sieciowa
	Możliwość odtworzenia	Regularna kontrola sprzętu [cykl życia, wydajność]
		Zarządzanie reakcją na incydenty
		Backup baz danych
		Weryfikacja możliwości odtworzenia
Procedury regularnego wykonywania przeglądu, walidacji i oceny	Zarządzanie ochroną danych	Koncepcja uprawnień
		Koncepcja kopii zapasowych
		Koncepcja odzyskiwania danych
		Zarządzanie reakcją na incydenty
		Polityka Ochrony Danych Osobowych
	Regularne kontrole i ewentualna optymalizacja	Regularne audyty prowadzone przez Inspektora Ochrony Danych
		Aktualizacja podejmowanych działań
	Ochrona danych w fazie projektowania oraz domyślna ochrona danych	Zatwierdzona procedura