KSIĘGA ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA

JAKOŚCIĄ, ŚRODOWISKIEM, BHP i BEZPIECZEŃSTWEM INFORMACJI w Spółce MGGP S.A.

Wersja 1.4

Wyciąg z dokumentacji ZSZ wdrożonego w MGGP S.A. w zakresie Bezpieczeństwa Informacji w MGGP S.A.
/dla Personelu współpracującego ze Spółką na podstawie innych stosunków prawnych niż umowa o pracę/

SPIS TREŚCI

KSIĘGA ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA **1**
SPIS TREŚCI **1**
Słownik do dokumentacji SZBI **2**
Procedura III.E.1 Polityka Ochrony Danych Osobowych **4**
Załącznik III.E.1-Z1 Zasady postępowania z informacjami w wersji papierowej 21
Procedura III.E.2 Instrukcja zarządzania systemem informatycznym **24**
Procedura III.E.4 Regulamin Użytkownika systemów informatycznych **30**
Załącznik III.E.4-Z1 Zasady bezpieczeństwa informacji 42
Procedura III.E.6 Bezpieczeństwo fizyczne **43**
Załącznik III.E.6-Z1 Zasady postępowania z kluczami i kartami dostępu do budynków/pomieszczeń MGGP S.A. 45
Klasyfikacja informacji w MGGP S.A. **47**

Słownik do dokumentacji SZBI

W dokumentach związanych z Bezpieczeństwem Informacji oraz Ochroną Danych Osobowych stosowane są następujące definicje:

	Administrator Danych Osobowych/ADO	Administrator Danych Osobowych: MGGP S.A. z siedzibą w 33-100 Tarnów, przy ulicy Kaczkowskiego 6, REGON: 490808053.
	Anonimizacja	Takie przetworzenie Danych, które powoduje trwałe pozbawienie możliwości przypisania ich do konkretnej osoby fizycznej.
	Administrator Systemu Informatycznego / ASI	Administrator Systemu Informatycznego – osoba wyznaczona przez ADO, mająca uprawnienia administracyjne w danym systemie informatycznym i odpowiedzialna za zapewnienie zgodności przetwarzania Danych Osobowych i innych danych istotnych dla organizacji z wdrożoną dokumentacją w zakresie SZBI oraz powszechnie obowiązującymi przepisami prawa. Nadzoruje zasoby informatyczne w Organizacji. Niektóre czynności w imieniu ASI mogą wykonywać upoważnieni przez niego Pracownicy Działu IT.
	Zastępca Administratora Systemu Informatycznego / Zastępca ASI	Zastępca Administratora Systemu Informatycznego – osoba wyznaczona przez ADO, podlegająca bezpośrednio pod ASI i wykonująca jego polecenia w zakresie praw i obowiązków ASI. Zastępuje ASI pod jego nieobecność, w tym czasie wszystkie prawa i obowiązki jakie posiada ASI i podlegając pod ADO.
	Archiwizacja	Proces służący zapewnieniu wieloletniego przechowywania dokumentów, a także danych w wersji elektronicznej, w sposób który umożliwi ich odczytanie. Archiwizacja obejmuje proces sortowania, katalogowania oraz nadawania kategorii, określającej okres przechowywania archiwizowanej dokumentacji.
	Bezpieczeństwo informacji i ochrona Danych Osobowych	Zapewnienie poufności, integralności, dostępności Danych Osobowych i innych danych istotnych dla organizacji oraz rozliczalności, poprzez wdrożenie i eksploatację niezbędnych do tego celu mechanizmów technicznych i procedur organizacyjnych.
	Dane Osobowe	Informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, czyli takiej, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
	Inne dane	Dane mające wartość dla Organizacji, które powinny być chronione w ramach systemu bezpieczeństwa informacji
	Hasło	Ciąg znaków literowych, cyfrowych lub innych służący uwierzytelnieniu Użytkownika.
	Identyfikator	Nadany przez ADO ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących Użytkownika.
	Incydent	Zbiór złożony z jednego lub więcej zdarzeń lub uwarunkowań związanych z naruszeniem bezpieczeństwa lub podejrzeniem naruszenia, wymagający podjęcia działania i rozwiązania powstałego problemu w celu utrzymania akceptowalnego poziomu ryzyka. Szczególnym rodzajem incydentu jest Naruszenie ODO.
	Integralność danych	Właściwość zapewniająca, że Dane Osobowe i inne dane istotne dla Organizacji nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
	Inspektor Ochrony Danych Osobowych / IOD	Inspektor Ochrony Danych Osobowych. Jeżeli u ADO zostanie ustanowiony IOD, wykonuje on zadania wynikające z przepisów prawa oraz zadania, które zgodnie z niniejszą dokumentacją SZBI powierzono Koordynatorowi ds. ODO.
	Koordynator ds. ODO	Koordynator do spraw Ochrony Danych Osobowych – wyraźnie upoważniony przez ADO Użytkownik, który wykonuje obowiązki w zakresie ochrony Danych Osobowych wskazane w Procedurach. Jeżeli u ADO nie zostanie ustanowiony Koordynator ds. ODO lub IOD, zadania, które zgodnie z niniejszą dokumentacją SZBI powierzono Koordynatorowi ds. ODO wykonuje ADO.
	Naruszenie ODO	Naruszenie ochrony Danych Osobowych – oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do Danych Osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
	Nośnik danych lub Nośnik	Fizyczny lub elektroniczny nośnik informacji, występujący w formie wewnętrznej (stacjonarnej) lub zewnętrznej (przenośnej) na którym zapisywane są Dane Osobowe i inne dane istotne dla Organizacji. Elektroniczne nośniki danych to m.in.: dyski zewnętrzne, pendrive, płyty CD/DVD, pamięci typu flash.
	Obszar przetwarzania	Obszar znajdujący się pod kontrolą ADO lub Procesora, który przeznaczony jest do Przetwarzania Danych Osobowych i innych danych istotnych dla Organizacji i który można objąć Zabezpieczeniami.
	Ocena Skutków	Przeprowadzana przez ADO w sytuacjach wskazanych w Procedurach ocena skutków planowanych lub wykonywanych operacji przetwarzania dla ochrony Danych Osobowych.
	Odbiorca	Jakakolwiek osoba fizyczna lub prawna, organ publiczny, jednostka organizacyjna lub inny podmiot zewnętrzny wobec ADO, któremu ujawnia się Dane Osobowe. Za odbiorcę nie uznaje się organu publicznego, jeżeli otrzymuje on Dane Osobowe w ramach konkretnego postępowania, zgodnie z przepisami mającymi zastosowanie stosownie do celów przetwarzania.
	Opiekun	Osoba (upoważniona w tym zakresie przez ADO) odpowiedzialna za współpracę z Osobą Trzecią, której nadawane jest upoważnienie do przetwarzania Danych Osobowych i innych danych istotnych dla Organizacji oraz dostęp do Systemu informatycznego przetwarzającego dane.
	Opis przepływu Danych	Opis sposobu przepływu Danych pomiędzy poszczególnymi systemami informatycznymi.
	Opis struktury zbiorów	Opis struktury zbiorów Danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.
	Organ Nadzorczy	Organ ustanowiony na mocy odpowiednich przepisów prawa polskiego do nadzorowania wykonywania obowiązków ADO w zakresie ochrony Danych Osobowych.
	Organizacja	MGGP S.A.
	Osoba Trzecia	Podmiot trzeci/strona trzecia (osoba fizyczna lub prawna, albo jednostka organizacyjna) inna niż PDO, ADO, Użytkownik lub Procesor.
	Osoba upoważniona	Użytkownik systemu informatycznego uprawniony do przetwarzania Danych Osobowych i innych danych istotnych dla Organizacji.
	Państwo trzecie	To państwo nie należące do Europejskiego Obszaru Gospodarczego.
	Personel	Wszystkie osoby, które wykonują prace na rzecz Organizacji. Uszczegółowienie: obejmuje pracowników (zatrudnionych na podstawie umowy o pracę) oraz osoby współpracujące na podstawie innych stosunków prawnych.

	Podmiot Danych Osobowych / PDO	Osoba fizyczna, której Dane Osobowe są przetwarzane zgodnie z procedurami bezpieczeństwa.
	Poufność Danych	To właściwość zapewniająca, że Dane nie są udostępniane nieupoważnionym podmiotom.
	Procedury	Procedury Bezpieczeństwa Przetwarzania Danych Osobowych i innych danych istotnych dla Organizacji obowiązujące u ADO.
	Procesor lub Podmiot Przetwarzający	Osoba fizyczna lub prawna, organ publiczny, jednostka organizacyjna lub inny podmiot, który przetwarza Dane Osobowe i inne dane istotne dla Organizacji w imieniu ADO.
	Przetwarzanie	Operacja lub zestaw operacji wykonywanych na Danych Osobowych lub zestawach Danych Osobowych i innych danych istotnych dla Organizacji w sposób zautomatyzowany lub niezautomatyzowany. Przetwarzaniem w szczególności jest: 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.
	Pseudonimizacja	Przetworzenie Danych Osobowych i innych danych istotnych dla Organizacji w taki sposób, by nie można ich było już przypisać konkretnej osobie, której Dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
	Rejestr Czynności Przetwarzania lub RCP	Rejestr czynności przetwarzania, za które odpowiada Administrator, prowadzony zgodnie z art. 30 RODO oraz Procedurami.
	RODO/ Rozporządzenie	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).
	Rozliczalność	To właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
	Sieć publiczna	To sieć publiczna w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne.
	Sieć telekomunikacyjna	To sieć w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne.
	System lub System informatyczny	Zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych, w tym Danych Osobowych.
	Środki techniczne i organizacyjne	Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych Danych Osobowych i innych danych istotnych dla Organizacji.
	Teletransmisja	To przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej.
	Umowa Powierzenia	Umowa regulująca zasady powierzania Danych Osobowych do Przetwarzania przez Podmiot Przetwarzający zgodna z wzorami stanowiącymi Załącznik III.E.1-F1 oraz Załącznik III.E.1-F13 do niniejszej Polityki.
	Umowa podpowierzenia	Umowa regulująca zasady dalszego powierzenia Danych Osobowych do przetwarzania przez Dalszy Podmiot Przetwarzający zgodna z wzorami stanowiącymi Załącznik III.E.1-F15 do niniejszej Polityki.
	Uprawnienie PDO	Uprawnienie przysługujące Podmiotowi Danych Osobowych zgodnie z obowiązującymi przepisami w zakresie Przetwarzania Danych Osobowych i wykonywane zgodnie z odpowiednią Procedurą.
	Urządzenie przenośne	Urządzenie przenośne (w szczególności laptop, tablet, smartfon) umożliwiające przetwarzanie Danych Osobowych i innych danych istotnych dla Organizacji.
	Usuwanie Danych	To zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
	Uwierzytelnienie	Działanie, którego celem jest weryfikacja deklarowanej tożsamości.
	Użytkownik	Osoba fizyczna upoważniona przez ADO do przetwarzania Danych Osobowych (bez względu na ich formę) i innych danych istotnych dla Organizacji.
	Użytkownik Systemu Informatycznego / Użytkownik systemu	Osoba, której został przydzielony przez ASI indywidualny identyfikator w systemie informatycznym w powiązaniu z niezbędnymi uprawnieniami dostępowymi w tym systemie.
	Wykaz zbiorów	Wykaz zbiorów Danych Osobowych i innych danych istotnych dla Organizacji wraz ze wskazaniem programów zastosowanych do przetwarzania tych Danych.
	Zabezpieczenia	Środek techniczny lub organizacyjny służący ochronie Danych, a w szczególności zapewnieniu ich integralności, poufności, dostępności i rozliczalności.
	Zbiór Danych Osobowych	Uporządkowany zestaw Danych Osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
	Zbiór innych danych	Uporządkowany zestaw Danych istotnych dla Organizacji dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
	Zespół ds. ODO	Zespół składający się z IOD, Koordynatora ds. ODO, ASI, Zastępcy ASI i prawnika wewnętrznego lub przedstawiciela kancelarii obsługującej ADO w zakresie RODO.
	Zgoda osoby, której Dane dotyczą	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.

Procedura III.E.1 Polityka Ochrony Danych Osobowych

Właściciel procesu: Zarząd			
Wersja: 03	Kategoria jawności: II (wewnętrzne)	Obowiązuje od: 01.02.2024 r.	Stron: 17

1. CEL I PRZEDMIOT PROCEDURY	Celem dokumentu jest: a. określenie ogólnych zasad bezpieczeństwa informacji i ochrony Danych Osobowych; b. realizacja obowiązków wynikających z wymagań prawa, tj. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE oraz przepisów ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, a polegających na wdrożeniu przez ADO dokumentacji przetwarzania danych osobowych. c. zapewnienie należytej ochrony Danych Osobowych będących w zasobach ADO, w szczególności odpowiedniej do zagrożeń i kategorii Danych Osobowych objętych ochroną. Zakres przedmiotowy stosowania niniejszej dokumentacji obejmuje wszystkie zbiory Danych Osobowych przetwarzane przez ADO, zarówno w formie elektronicznej, jak i papierowej, oraz Dane Osobowe przetwarzane poza zbiorami Danych. Zakres podmiotowy stosowania niniejszej dokumentacji obejmuje wszystkich pracowników oraz osoby/podmioty, przy pomocy których ADO wykonuje swoje czynności, mające dostęp do Danych Osobowych lub innych wrażliwych informacji.
2. UCZESTNICY I ROLE W PROCEDURZE	**a) Administrator Danych Osobowych (ADO):** - zapewnia odpowiednie środki organizacyjne i techniczne celem przetwarzania danych osobowych zgodnie z określonymi w RODO zasadami przetwarzania danych osobowych, - wdraża odpowiednie procedury ochrony danych osobowych, - zapewnienia środki umożliwiające prawidłową realizację praw osób, których dane dotyczą, - zapewnia dopuszczenie do przetwarzania danych osobowych wyłącznie osób posiadających upoważnienie do przetwarzania danych osobowych, - zapewnia przetwarzanie danych osobowych wyłącznie na polecenie ADO, chyba że przetwarzanie wymagane jest przepisami prawa UE lub państwa członkowskiego, - wyznacza Koordynatora ds. ODO, udziela mu upoważnienia do nadawania personelowi upoważnień do przetwarzania danych osobowych, - wyznacza pracowników odpowiedzialnych m.in. za prowadzenie ewidencji osób upoważnionych, rejestru czynności przetwarzania, rejestru kategorii czynności przetwarzania rejestru umów powierzenia przetwarzania danych osobowych oraz rejestru wszelkich naruszeń ochrony danych osobowych, - współpracuje z organem nadzorczym, - zawiadamia o naruszeniu ochrony danych osobowych właściwy organ nadzorczy, a w przypadku, gdy zajdą ku temu odpowiednie przesłanki, zgłasza naruszenie osobie, której dane dotyczą, - wyznacza Administratora Systemów Informatycznych (ASI); **b) Koordynator ds. ODO:** - sprawuje bezpośredni nadzór nad wykonywaniem obowiązków wynikających z Procedur i Polityk RODO, - dba o aktualizację Procedur i rejestru czynności przetwarzania, - przygotowuje i przedstawia ADO do zatwierdzenia projekty zmian do Procedur oraz nowych dokumentów w ramach Procedur, - podejmuje odpowiednie działania w przypadku naruszenia ODO lub podejrzenia wystąpienia naruszenia ODO, - zapewnia zapoznanie wszystkich osób przetwarzających dane osobowe w imieniu ADO z treścią ich obowiązków wynikających z właściwych przepisów i Procedur, - nadaje upoważnienia do przetwarzania danych osobowych oraz prowadzi ewidencje osób upoważnionych do przetwarzania danych osobowych, rejestr czynności przetwarzania oraz rejestru kategorii czynności przetwarzania, rejestr umów powierzenia przetwarzania danych osobowych, - przeprowadzi audyty w zakresie przestrzegania RODO i wdrożonych procedur ochrony danych osobowych, - rozstrzyga, czy dana sytuacja obejmuje powierzenie danych osobowych do przetwarzania oraz odpowiada za zamieszczenie w Umowie Powierzenia lub wykorzystywanym instrumencie prawnym, informacji wymaganych zgodnie ze wzorem Umowy Powierzenia lub Klauzul Powierzenia, - podejmuje decyzję o powierzeniu lub przyjęciu danych osobowych do przetwarzania, - wykonuje w imieniu ADO żądania osób, których dane dotyczą w zakresie realizacji ich praw, - zawiadamia w imieniu ADO o naruszeniu ochrony danych osobowych właściwy organ nadzorczy, a w przypadku, gdy zajdą ku temu odpowiednie przesłanki, zgłasza naruszenie osobie, której dane dotyczą; **c) Administrator Systemów Informatycznych (ASI):** - odpowiada za zapewnienie przestrzegania zasad ochrony danych osobowych przetwarzanych za pomocą systemów informatycznych, - nadzoruje funkcjonowanie systemów informatycznych oraz zabezpieczeń, - przydziela i zarządza uprawnieniami Użytkowników do dostępu do systemów, - dba o aktualizację, sprawdzenia, wymianę oraz utylizację urządzeń, programów i narzędzi programowych w ramach systemów informatycznych, - przygotowuje i przedstawia ADO do zatwierdzenia propozycje zmian w ramach systemów i zabezpieczeń, - współdziała z Koordynatorem ODO w przypadku naruszenia ODO lub podejrzenia wystąpienia naruszenia ODO, - współdziała z Koordynatorem ODO w przypadku wystąpienia przez PDO z żądaniami w ramach Uprawnień PDO; **d) Dyrektorzy/Menadżerowie/Liderzy/Kierownicy Projektu:** - zarządzają czynnościami przetwarzania danych osobowych w ramach zadań, realizowanych przez swoje jednostki organizacyjne, - występują z wnioskami do ASI o nadanie, zmianę lub cofniecie uprawnień personelowi do określonych zasobów danych osobowych przetwarzanych w systemie informatycznym, zgodnie z zakresem upoważnienia do przetwarzania danych osobowych,

	- występują z wnioskami do Koordynatora ds. ODO o nadanie, zmianę lub cofniecie upoważnień do przetwarzania danych osobowych personelowi, który wykonując zadania służbowe przetwarza dane osobowe, - zapoznają podległy personel i inne osoby (np. współpracowników) z zasadami przetwarzania i ochrony danych w podległej jednostce organizacyjnej, - wypełniają obowiązki dotyczące zabezpieczenia obszaru przetwarzanych danych osobowych w podległej jednostce organizacyjnej, - zgłaszają do ASI zamiar rozpoczęcia nowego procesu przetwarzania danych osobowych lub zmiany w czynnościach przetwarzania danych realizowanych w jednostce organizacyjnej, - w przypadku zbierania danych osobowych, konsultują z koordynatorem ds. ODO podstawy prawne przetwarzania danych osobowych, w tym zbierania i archiwizowanie zgód osób na przetwarzanie ich danych osobowych w wymaganych przypadkach, - ustalają w porozumieniu z ASI zasady tworzenia kopii zapasowych plików z danymi osobowymi, znajdującymi się na stacjach roboczych użytkowników w podległej jednostce organizacyjnej, - przechowują nadane upoważnienia do przetwarzania danych osobowych oraz oświadczenia o zachowaniu tajemnicy danych osobowych i sposobów ich zabezpieczania, - powiadamiają Koordynatora ds. ODO o zgłoszeniu żądania w zakresie realizacji praw osób, których dane dotyczą; **e) Personel, w tym w szczególności osoby upoważnione do przetwarzania danych osobowych:** - zapoznają się z przepisami prawa w zakresie ochrony danych osobowych, w tym przepisami Polityki służącymi do przetwarzania danych osobowych, - stosują określone przez Administratora procedury oraz wytyczne mające na celu zgodne z prawem, w tym zwłaszcza adekwatne, przetwarzanie danych, - odpowiednio zabezpieczają dane przed ich udostepnieniem osobom nieupoważnionym, - informują Administratora niezwłocznie od powzięcia wiedzy o wszelkich podejrzeniach naruszenia lub stwierdzonych naruszeniach oraz wadach systemu przetwarzającego dane osobowe, - zawiadamiają Koordynatora ODO o sytuacjach, które mogą wymagać powierzenia danych osobowych do przetwarzania lub przyjęcia danych osobowych do przetwarzania od innego administratora, - zawiadamiają ASI oraz Koordynatora ODO o zamiarze wykorzystania nowego systemu informatycznego służącego przetwarzaniu danych osobowych, - jeżeli przed przystąpieniem lub w trakcie przetwarzania danych stwierdzają, że dane otrzymane do przetwarzania od innego podmiotu niż podmiot danych osobowych stanowią dane osobowe, zgłaszają zaistniałą sytuację do Koordynatora ODO, - powiadamiają bezpośredniego przełożonego w strukturze organizacyjnej ADO o zgłoszeniu żądania w zakresie realizacji praw osób, których dane dotyczą.
3. TERMINOLOGIA	Definicje stosowane w niniejszym dokumencie zawarte są w słowniku.
4. INSTRUKCJE POSTĘPOWANIA	
Nr 4.1	**Ustalenie kontekstu, identyfikacja zainteresowanych stron oraz ocena ryzyka** 1.1.1. W celu określenia Polityki ochrony Danych Osobowych należy we właściwy sposób ustalić kontekst (czyli środowisko, w którym Organizacja stara się osiągnąć swoje cele) oraz oszacować ryzyko. Działanie te są wykonywane zgodnie z *Procedurą III.E.3 Zarządzanie ryzykiem dotyczącym bezpieczeństwa informacji i ochrony Danych Osobowych*.
Nr 4.2	**Postanowienia ogólne dotyczące ochrony Danych Osobowych** 1.2.1. Postanowienia ogólne dotyczące ADO. 1.2.1.1. W celu zapewnienia ochrony przetwarzanych Danych Osobowych zarówno za pomocą systemów informatycznych jak i w wersji papierowej oraz spełnienia wymogów art. 24 ustawy RODO, ADO wdraża niniejszą Politykę ochrony Danych Osobowych, będącą aktualizacją dotychczas obowiązujących dokumentów dotyczących przetwarzania Danych Osobowych. W zakresie dokumentacji papierowej obowiązują dodatkowo zasady opisane w *Załączniku III.E.1-Z1 Zasady postępowania z informacjami w wersji papierowej*. 1.2.1.2. ADO dokłada należytej staranności w celu ochrony interesów osób, których Dane Osobowe dotyczą, w szczególności jest obowiązany zapewnić, aby Dane były przetwarzane zgodnie z zasadami wskazanymi w RODO i w niniejszej polityce bezpieczeństwa i musi być w stanie wykazać ich przestrzeganie („rozliczalność"). 1.2.1.3. ADO deklaruje pełne zaangażowanie i determinację celem zapewnienia bezpieczeństwa przetwarzanych Danych Osobowych, a także prawidłowego zabezpieczenia systemu informatycznego służącego do przetwarzania Danych Osobowych. 1.2.1.4. ADO nadzoruje jakie Dane, kiedy i przez kogo zostały do zbiorów ADO wprowadzone, bądź z tych zbiorów usunięte oraz komu są przekazywane, a także jakie Dane przetwarzane są poza zbiorami Danych. 1.2.1.5. ADO na bieżąco dostosowuje systemy informatyczne służące do przetwarzania Danych i wszelkie systemy zabezpieczeń przetwarzania Danych Osobowych do wymogów określonych w rozporządzeniu. 1.2.2. Postanowienia ogólne dotyczące przetwarzania. 1.2.2.1. Wszelkie przetwarzanie Danych Osobowych powinno być zgodne z prawem i rzetelne. 1.2.2.2. Dla osób fizycznych powinno być przejrzyste, że dotyczące ich Dane Osobowe są zbierane, wykorzystywane, przeglądane lub w inny sposób przetwarzane oraz w jakim stopniu te Dane Osobowe są lub będą przetwarzane. Zasada przejrzystości wymaga, by wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem tych Danych Osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem. Zasada ta obejmuje w szczególności informowanie osób, których Dane dotyczą, o tożsamości ADO i celach przetwarzania oraz przekazywanie innych informacji mających zapewnić rzetelność i przejrzystość przetwarzania w stosunku do osób, których sprawa dotyczy, a także prawa takich osób do uzyskania potwierdzenia i informacji o przetwarzanych Danych Osobowych ich dotyczących, w tym prawa do otrzymania kopii ich Danych Osobowych.
	1.2.2.3. Osobom fizycznym należy uświadomić ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem Danych Osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem. W szczególności konkretne cele przetwarzania Danych Osobowych powinny być wyraźne, uzasadnione i określone w momencie ich zbierania.

	1.2.2.4. Dane Osobowe powinny być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane. Wymaga to w szczególności zapewnienia ograniczenia okresu przechowywania Danych do ścisłego minimum. 1.2.2.5. Dane Osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami. Aby zapobiec przechowywaniu Danych Osobowych przez okres dłuższy, niż jest to niezbędne, ADO powinien ustalić termin ich usuwania lub okresowego przeglądu. 1.2.2.6. Należy podjąć wszelkie rozsądne działania zapewniające sprostowanie lub usunięcie Danych Osobowych, które są nieprawidłowe. 1.2.2.7. ADO zobowiązany jest zapewnić również integralność i poufność przetwarzanych Danych Osobowych, to jest by Dane te były przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo Danych Osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych. 1.2.2.8. Wszelkie czynności jakie na mocy niniejszej Polityki bezpieczeństwa są wykonywane przez Koordynatora ds. ODO lub ASI mogą być także wykonywane przez ADO.
Nr 4.3	**Administrator Danych Osobowych (ADO)** 4.3.1 ADO, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, ADO uwzględnia w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do Danych Osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. 4.3.2. ADO w szczególności zapewnia: a) środki techniczne i organizacyjne niezbędne dla zapewnienia bezpiecznego przetwarzania Danych w pomieszczeniach do tego przeznaczonych; b) system i sprzęt informatyczny umożliwiający bezpieczne przetwarzanie danych; c) dopuszczenie do przetwarzania Danych Osobowych wyłącznie osób posiadających upoważnienie do przetwarzania Danych Osobowych; d) przetwarzanie Danych Osobowych wyłącznie na polecenie ADO, chyba że przetwarzanie wymagane jest przepisami prawa UE lub państwa członkowskiego; e) zapoznanie z przepisami o ochronie Danych Osobowych każdej osoby upoważnionej do przetwarzania Danych Osobowych; f) prowadzenie ewidencji osób upoważnionych; g) należyte i terminowe udzielanie informacji na wniosek osób, których Dane są przetwarzane i które zwróciły się z wnioskiem o udzielenie informacji; h) kontrolę nad tym jakie Dane, kiedy i przez kogo są przetwarzane, w tym zbierane, usuwane oraz komu i przez kogo przekazane. 4.3.3. Do obowiązków ADO należy także prowadzenie rejestru czynności przetwarzania oraz rejestru kategorii czynności przetwarzania tam, gdzie występuje jako Podmiot Przetwarzający. 4.3.4. W razie wystąpienia przez Podmiot Danych Osobowych z żądaniem skorzystania z Uprawnień PDO, ADO zobowiązany jest podjąć niezbędne środki, aby wykonać to żądanie, po uprzedniej weryfikacji, czy jest ono zgodne z przepisami, a także z uwzględnieniem wymagań czasowych dla jego realizacji wynikających z przepisów. 4.3.5. ADO jest obowiązany poinformować bez zbędnej zwłoki innych administratorów, którym udostępnił zbiór Danych, o dokonanym uaktualnieniu lub sprostowaniu Danych. 4.3.6. ADO zobowiązany jest uwzględniać ochronę Danych już w fazie projektowania (planowania), to jest biorąc pod uwagę okoliczności wskazane w punkcie 4.8.1 wdrażać odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane (zaplanowane) w celu skutecznej realizacji zasad Ochrony Danych, takich jak minimalizacja Danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi z przepisów oraz chronić prawa osób, których Dane dotyczą. 4.3.7. Administrator zobowiązany jest uwzględniać zasadę domyślnej ochrony Danych, to jest wdrażać odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te Dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych Danych Osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie Dane Osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.
Nr 4.4	**Koordynator ds. ODO, Inspektor Ochrony Danych (IOD) i Administrator Systemu Informatycznego (ASI).** 3.1.1. Powołanie Koordynatora ds. ODO. 3.1.1.1. ADO może wyznaczyć na Koordynatora ds. ODO osobę, która posiada odpowiednią wiedzę w zakresie ochrony Danych Osobowych. 3.1.1.2. W dokumencie powołującym Koordynatora ds. ODO osoba powołana do pełnienia tej funkcji musi być wskazana z imienia i nazwiska. 3.1.1.3. ADO może powierzyć Koordynatorowi ds. ODO wykonywanie innych obowiązków z zakresu ochrony Danych niż wskazane wprost w niniejszej Polityce bezpieczeństwa. 3.1.1.4. Koordynator ds. ODO podlega bezpośrednio Zarządowi ADO. 3.1.1.5. ADO zapewnia środki i organizacyjną odrębność Koordynatora ds. ODO niezbędne do niezależnego wykonywania przez niego zadań. 3.1.2. Obowiązki Koordynatora ds. ODO. 3.1.2.1. Koordynator ds. ODO sprawuje bezpośredni nadzór nad wykonywaniem obowiązków wynikających z Procedur i Polityk.

	3.1.2.2. Koordynator zapoznaje się na bieżąco ze zmianami przepisów w zakresie ochrony Danych Osobowych i wytycznymi Organu Nadzorczego. 3.1.2.3. Koordynator ds. ODO dba o aktualizację Procedur i rejestru czynności przetwarzania, przygotowuje i przedstawia ADO do zatwierdzenia projekty zmian do Procedur oraz nowych dokumentów w ramach Procedur. 3.1.2.4. Koordynator ds. ODO podejmuje odpowiednie działania w przypadku Naruszenia ODO lub podejrzenia wystąpienia Naruszenia ODO. 3.1.2.5. Koordynator ds. ODO zapewnia zapoznanie wszystkich osób przetwarzających Dane Osobowe w imieniu ADO z treścią ich obowiązków wynikających z właściwych przepisów i Procedur. 3.1.2.6. Koordynator prowadzi ewidencję Użytkowników upoważnionych do przetwarzania Danych Osobowych, dbając by zakres upoważnień odpowiadał zakresowi obowiązków Użytkowników. 3.1.3. Powołanie Inspektora Ochrony Danych. 3.1.3.1. ADO może wyznaczyć i zgłosić do rejestru (prowadzonego przez Prezesa Urzędu Ochrony Danych Osobowych) Inspektora Ochrony Danych (IOD), który jest odpowiedzialny za przetwarzanie Danych zgodnie z ustawą oraz rozporządzeniem. 3.1.3.2. Zgłoszenia, o którym mowa powyżej dokonuje się według wzoru określonego w Ustawie o ochronie danych osobowych. 3.1.3.3. ADO może wyznaczyć co najmniej jednego zastępcę IOD. Zastępca IOD musi spełniać wszystkie wymagania określone w aktualnych przepisach dot. ochrony Danych Osobowych. 3.1.3.4. Zastępca IOD wykonuje wszystkie obowiązki należące do zakresu obowiązków IOD podczas jego nieobecności. 3.1.4. Obowiązki Inspektora Ochrony Danych. 3.1.4.1. W przypadku wyznaczenia IOD oraz zgłoszenia IOD do rejestru prowadzonego przez Prezesa Urzędu Ochrony Danych Osobowych, do zadań IOD należy: a) informowanie ADO oraz Użytkowników, którzy przetwarzają Dane Osobowe, o obowiązkach spoczywających na nich na mocy RODO, innych przepisów Unii Europejskiej lub polskich o ochronie Danych, Procedur i doradzanie im w tej sprawie, b) monitorowanie przestrzegania RODO, innych przepisów Unii lub polskich o ochronie Danych oraz Procedur, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty, c) udzielanie na żądanie zaleceń co do Oceny skutków dla ochrony Danych oraz monitorowanie jej wykonania, d) współpraca z organem nadzorczym (Prezesem Urzędu Ochrony Danych Osobowych), e) pełnienie funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach. 3.1.4.2. W celu sprawnej realizacji nałożonych zadań, IOD przysługują uprawnienia określone w Ustawie. 3.1.5. Kompetencje Inspektora Ochrony Danych. 3.1.5.1. IOD jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie Ochrony Danych oraz umiejętności wypełnienia zadań. 3.1.5.2. W dokumencie powołującym IOD osoba powołana do pełnienia funkcji IOD musi być wskazana z imienia i nazwiska. 3.1.5.3. ADO może powierzyć IOD wykonywanie innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania przez IOD obowiązków i nie powoduje konfliktu interesów. 3.1.5.4. IOD podlega bezpośrednio Zarządowi ADO. 3.1.5.5. ADO zapewnia środki i organizacyjną odrębność IOD niezbędne do niezależnego wykonywania przez niego zadań. 3.1.6. Powołanie Administratora Systemów Informatycznych (ASI). 3.1.6.1. Administrator może wyznaczyć Administratora Systemów Informatycznych. 3.1.6.2. ASI wykonuje następujące obowiązki: a) odpowiada za zapewnienie przestrzegania zasad ochrony Danych Osobowych przetwarzanych za pomocą systemów informatycznych zgodnie z *Procedurą III.E.2 Instrukcja zarządzania systemem informatycznym*, b) nadzoruje funkcjonowanie systemów informatycznych oraz zabezpieczeń, c) przydziela i zarządza uprawnieniami Użytkowników do dostępu do systemów, d) dba o aktualizację, sprawdzenia, wymianę oraz utylizację urządzeń, programów i narzędzi programowych w ramach systemów informatycznych, e) przygotowuje i przedstawia ADO do zatwierdzenia propozycje zmian w ramach systemów i zabezpieczeń, f) współdziała z Koordynatorem ODO w przypadku Naruszenia ODO lub podejrzenia wystąpienia Naruszenia ODO, g) współdziała z Koordynatorem ODO w przypadku wystąpienia przez PDO z żądaniami w ramach Uprawnień PDO. 3.1.6.3. ASI podczas wykonywania obowiązków z zakresu ochrony Danych Osobowych podlega bezpośrednio ADO. 3.1.6.4. W przypadku niewyznaczenia ASI za zapewnienie przestrzegania zasad ochrony Danych Osobowych przetwarzanych za pomocą systemów informatycznych odpowiada ADO.
Nr 4.5	**Przetwarzanie Danych Osobowych** 1.5.1. Podstawy przetwarzania Danych Osobowych. 1.5.1.1. Przetwarzanie Danych jest dopuszczalne tylko wtedy, gdy: a) PDO wyraził zgodę na przetwarzanie swoich Danych Osobowych w jednym lub większej liczbie określonych celów,

b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest PDO lub do podjęcia działań na żądanie PDO przed zawarciem umowy,
c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na ADO,
d) przetwarzanie jest niezbędne do ochrony żywotnych interesów PDO, lub innej osoby fizycznej,
e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej ADO,
f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez ADO lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której Dane dotyczą, wymagające ochrony Danych Osobowych, w szczególności gdy osoba, której Dane dotyczą, jest dzieckiem.

1.5.1.2. Za prawnie uzasadniony cel ADO uznaje się w szczególności dochodzenie roszczeń z tytułu prowadzonej działalności oraz obronę przed takimi roszczeniami, zapobieganie i ochronę przed oszustwami i innymi czynami niedozwolonymi przeciwko ADO oraz marketing bezpośredni własnych produktów lub usług, przy czym przy podejmowaniu działań marketingowych za pomocą środków komunikacji elektronicznej należy stosować przepisy ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną oraz ustawy z dnia 16 lipca 2004 r. prawo telekomunikacyjne, które przewidują dalej idącą ochronę.

1.5.2. Zgoda na przetwarzanie.

1.5.2.1. Zgoda na przetwarzanie Danych Osobowych, nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

1.5.2.2. Zgoda to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba której Dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie jej Danych Osobowych.

1.5.2.3. Zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeśli przetwarzanie służy różnym celom, zgoda powinna wyraźnie określać wszystkie z nich. Jeżeli osoba, której Dane dotyczą, ma udzielić zgody w odpowiedzi na zapytanie elektroniczne lub telefoniczne, zapytanie takie musi być jasne, zwięzłe i nie zakłócać niepotrzebnie korzystania z usługi/działań, której dotyczy.

1.5.2.4. Dalsze przetwarzanie Danych w innym celu, niż ten, w którym Dane zostały zebrane, w oparciu o podstawę prawną inną niż zgoda lub przepis prawa, w tym w szczególności w oparciu o prawnie uzasadniony interes, może następować tylko, jeżeli ADO weźmie pod uwagę:
a) wszelkie związki między celami, w których zebrano Dane Osobowe, a celami zamierzonego dalszego przetwarzania,
b) kontekst, w którym zebrano Dane Osobowe, w szczególności relację między osobami, których Dane dotyczą a ADO,
c) charakter Danych Osobowych, w szczególności czy przetwarzane są szczególne kategorie Danych Osobowych lub Dane Osobowe dotyczące wyroków skazujących i naruszeń prawa,
d) ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których Dane dotyczą,
e) istnienie odpowiednich zabezpieczeń, w tym ewentualnie szyfrowania lub pseudonimizacji.

1.5.2.5. Zgoda na przetwarzanie Danych Osobowych może zostać wycofana w każdym czasie. W przypadku odwołania zgody na przetwarzanie Danych Osobowych, ADO obowiązany jest usunąć wszystkie Dane Osobowe osoby, która zgodę cofnęła, chyba że istnieje inna podstawa prawna upoważniająca ADO do dalszego przetwarzania tych Danych dla innych celów niż wskazany w cofniętej zgodzie. Wycofanie zgody nie wpływa na zgodność z prawem Przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem, o czym osoba, której Dane dotyczą, jest informowana zanim wyrazi zgodę. ADO zapewnia, by wycofanie zgody było równie łatwe jak jej wyrażenie.

1.5.2.6. Zaleca się odbieranie zgody w postaci możliwej do późniejszego udowodnienia (np. pisemnie, w ramach systemu informatycznego po zastosowaniu metody dwustopniowego uwiarygodniania, jako nagranie przeprowadzonej rozmowy telefonicznej – po poinformowaniu rozmówcy o prowadzonej rejestracji).

1.5.2.7. Każdorazowo, w przypadku zamiaru przystąpienia do zbierania Danych Osobowych w nowy sposób należy przestrzegać zasad „privacy by design" wskazanych w punkcie 4.8 Zaleca się, aby w przypadku tworzenia nowych wzorców zgody uzyskiwać opinię na temat treści zgody u IOD.

1.5.3. Obowiązek informacyjny.

1.5.3.1. ADO ma obowiązek poinformować wszystkie Podmioty Danych Osobowych o fakcie przetwarzania Danych Osobowych. W zależności od sytuacji może być to realizowane poprzez:
a) zawarcie odpowiednich klauzul w umowie,
b) umieszczenie informacji w ogólnie dostępnych miejscach lub na stronie internetowej,
c) osobiste przekazanie informacji,
d) przekazanie informacji mailowo, listownie lub poprzez osoby upoważnione.

1.5.3.2. Klauzule informacyjne powinny spełniać aktualne wymagania przepisów w zakresie ochrony Danych Osobowych. Wzory klauzul są zawarte w *Formularzach III.E.1-F14 od a do f.*

1.5.4. Przetwarzanie danych na stronach www.

1.5.4.1. W przypadku przetwarzania danych osobowych udostępnionych na stronach www należących do ADO, obowiązują dodatkowo zapisy *Polityki prywatności i Polityki Cookies (Załącznik III.E.1-Z2)*.

1.5.5. Postępowanie w sytuacjach wątpliwych i prawnie niejasnych.

1.5.5.1. W przypadku powzięcia jakichkolwiek wątpliwości co do ewentualnej zgodności z prawem planowanych działań w zakresie przetwarzania Danych, należy zwrócić się do Koordynatora ds. ODO z wnioskiem o rozstrzygnięcie wątpliwości.

1.5.5.2. Przed udzieleniem przez Koordynatora ds. ODO odpowiedzi w przedmiocie istniejących wątpliwości niedozwolone jest zbieranie Danych Osobowych i ich utrwalanie, a w przypadku posiadania już Danych Osobowych, których wątpliwość dotyczy należy, do czasu rozstrzygnięcia wątpliwości, wstrzymać wszystkie działania na Danych Osobowych, co do których istnieją wątpliwości czy są prawnie uzasadnione.

Nr 4.6

Powierzenie Przetwarzania Danych

4.6.1 ADO może powierzyć przetwarzanie Danych innemu podmiotowi, w drodze umowy, upoważnienia lub innego instrumentu prawnego zawartych na piśmie lub w formie elektronicznej.

4.6.2 Podmiot, któremu Dane do przetwarzania powierzono, może przetwarzać Dane wyłącznie w zakresie i w celu przewidzianym w ww. umowie lub instrumencie prawnym.

4.6.3 Podmiot, któremu powierzono przetwarzanie Danych obowiązany jest przed rozpoczęciem przetwarzania Danych podjąć środki zabezpieczające przetwarzanie Danych, o których mowa w Rozporządzeniu.

4.6.4 Zlecanie podmiotom zewnętrznym jakichkolwiek czynności związanych z przekazaniem i przetwarzaniem Danych Osobowych w imieniu ADO, w sytuacji, gdy administratorem Danych pozostaje ADO, stanowi powierzenie Danych Osobowych do przetwarzania.

4.6.5 Ilekroć dojdzie do zidentyfikowania sytuacji, która wymagać może powierzenia Danych Osobowych do przetwarzania, lub przyjęcia Danych Osobowych do przetwarzania od innego administratora, Użytkownik, który taką informację poweźmie, zawiadamia o tym Koordynatora ds. ODO.

4.6.6 Koordynator ds. ODO rozstrzyga, czy dana sytuacja obejmuje powierzenie Danych Osobowych do prtwarzania i w takiej sytuacji zawiadamia ADO lub osobę upoważnioną przez ADO do decydowania o powierzeniu Danych Osobowych.

4.6.7 ADO, po zasięgnięciu opinii Koordynatora ds. ODO zobowiązany jest ocenić, czy z danym powierzeniem lub przyjęciem Danych Osobowych do przetwarzania wiąże się obowiązek przeprowadzenia Oceny Skutków dla Ochrony Danych, stosując w tym celu metodykę szacowania ryzyka określoną w *Procedurze III.E.3 Zarządzanie ryzykiem dotyczącym bezpieczeństwa informacji i ochrony Danych Osobowych*.

4.6.8 Decyzję o powierzeniu lub przyjęciu Danych Osobowych do przetwarzania podejmuje ADO lub upoważniona w tym zakresie osoba.

4.6.9 Dokonując wyboru podmiotu zewnętrznego, któremu powierzone mają zostać Dane Osobowe do przetwarzania, ADO dokonuje weryfikacji, czy daje on wystarczające gwarancje wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom prawa, w tym w zakresie bezpieczeństwa przetwarzania, w szczególności jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby.

4.6.10 Powierzenie lub przyjęcie Danych Osobowych do przetwarzania odbywa się na podstawie Umowy Powierzenia lub innego instrumentu zawierającego Klauzule powierzenia, zawartych na piśmie lub w formie elektronicznej pomiędzy ADO, a podmiotem trzecim, któremu zleca się czynności, związane z przetwarzaniem Danych Osobowych lub który takie czynności zleca ADO.

4.6.11 W przypadku powierzenia danych wewnątrz krajów UE należy stosować *Umowę Powierzenia (Formularz III.E.1-F1)*. W przypadku powierzenia Danych do państw trzecich należy stosować klauzule opisane w *Formularzu III.E.1-F13*.

4.6.12 Koordynator ds. ODO odpowiada za zamieszczenie w Umowie Powierzenia lub wykorzystywanym instrumencie prawnym, informacji wymaganych zgodnie ze wzorem Umowy Powierzenia lub Klauzul Powierzenia, w tym w szczególności wskazanie: przedmiotu i czasu trwania przetwarzania, charakteru i celu przetwarzania, rodzaju Danych Osobowych oraz kategorii osób, których Dane dotyczą, obowiązków i praw ADO, a także uregulowanie ewentualnego dopuszczenia korzystania z dalszych podmiotów przetwarzających Dane Osobowe w ramach tej umowy/instrumentu prawnego (wraz z podaniem ich pełnej nazwy, adresu i danych kontaktowych).

4.6.13 Projekt umowy dotyczącej powierzenia Danych Osobowych do przetwarzania podmiotowi trzeciemu lub przyjęcia Danych Osobowych od podmiotu trzeciego do przetwarzania, który nie został przygotowany zgodnie ze Wzorem Umowy Powierzenia, wymaga każdorazowo akceptacji ADO, która poprzedzona winna być konsultacją z Koordynatorem ODO i Działem Prawnym pod kątem zgodności z przepisami prawa powszechnie obowiązującego oraz niniejszą Polityką.

4.6.14 Podpisanie Umowy Powierzenia Danych Osobowych do przetwarzania podmiotowi trzeciemu lub podpisanie Umowy powierzenia Danych Osobowych w sytuacji przyjęcia do przetwarzania Danych osobowych od podmiotu trzeciego, Koordynator ds. ODO odnotowuje w *Rejestrze Umów Powierzenia (Formularz III.E.1-F2)*, który zawiera informacje o: stronach takiej umowy oraz danych IOD, jeżeli został ustanowiony, zakresie Danych Osobowych objętych umową i czynności dokonywanych na Danych, czasie trwania, częstotliwości wykonywania audytów w ramach Umowy, dalszych podmiotach przetwarzających Dane Osobowe w ramach tej Umowy (wraz z podaniem ich pełnej nazwy, adresu i danych kontaktowych), fakcie przekazania Danych Osobowych do Państwa Trzeciego lub do organizacji międzynarodowej oraz opis (lub wskazanie miejsca, gdzie dostępna jest dokumentacja) zastosowanych w takiej sytuacji zabezpieczeń, o których mowa w art. 46 RODO i ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, a także kopię zawartej Umowy oraz informację o zakończeniu trwania Umowy i wykonaniu obowiązku usunięcia lub zwrócenia Danych Osobowych, albo dalszej podstawie przetwarzania ich przez podmiot trzeci.

4.6.15 Po zakończeniu trwania okresu przetwarzania Danych Osobowych powierzonych podmiotowi trzeciemu Koordynator ds. ODO weryfikuje, czy podmiot ten zwrócił lub usunął Dane Osobowe, chyba że przepisy prawa, którym podlega podmiot przetwarzający, nakładają obowiązek przechowywania Danych Osobowych.

4.6.16 Przekazania Danych do państwa trzeciego jest możliwe, jeżeli Komisja Europejska stwierdzi, że Państwo to zapewnia odpowiedni stopień ochrony (art. 45 RODO) lub jeżeli zastosowane zostaną odpowiednie zabezpieczenia, o których mowa w art. 46 RODO. Jeżeli przekazanie nie może się opierać na art. 45 ani 46 RODO, ADO weryfikuje, czy następuje jeden z wyjątków wskazanych w art. 49 RODO, a decydując się w takiej sytuacji na przekazanie, informuje osoby, których Dane dotyczą, o takim przekazaniu i o ważnych prawnie uzasadnionych interesach realizowanych przez ADO.
W przypadku powierzenia Danych do państw trzecich należy podpisać z podmiotem przetwarzającym umowę, która powinna zawierać wszystkie klauzule opisane w *Formularzu III.E.1-F13*. Poza tym wymagane jest wypełnienie:
Dodatku nr 1 – zawierającego m.in. opis podmiotów, kategorie Danych i czynności przetwarzania,
Dodatku nr 2 – zawierającego opis środków bezpieczeństwa

4.6.17 MGGP S.A. jako podmiot przetwarzający może powierzyć dalsze powierzenie przetwarzania danych osobowych tylko i wyłącznie wtedy, kiedy uzyska uprzednio szczegółową lub ogólną zgodę administratora danych na piśmie lub w formie elektronicznej. Dopuszczalna jest również forma dokumentu uzyskania zgody, o której mowa w art.77^2 kc (forma dokumentowa jest to złożenie oświadczenia woli w postaci nośnika informacji, w sposób

	umożliwiający ustalenie osób składających oświadczenie oraz zapoznanie się z całą treścią oświadczenia. Nośnikiem tym będzie więc e-mail, sms, zapis dźwięku i obrazu). 4.6.18 Na podstawie zgody, o której mowa w pkt 4.6.17 powyżej, MGGP S.A. może powierzyć dalsze powierzenie przetwarzania danych osobowych, w drodze umowy, upoważnienia lub innego instrumentu prawnego zawartych na piśmie lub w formie elektronicznej. 4.6.19 Podmiot, któremu powierzono dalsze przetwarzanie danych osobowych, może przetwarzać Dane wyłącznie w zakresie i w celu przewidzianym w ww. umowie lub instrumencie prawnym. 4.6.20 Podmiot, któremu powierzono dalsze przetwarzanie danych osobowych obowiązany jest przed rozpoczęciem przetwarzania Danych podjąć środki zabezpieczające przetwarzanie Danych, o których mowa w Rozporządzeniu. 4.6.21 Ilekroć dojdzie do zidentyfikowania sytuacji, która wymagać może dalszego powierzenia przetwarzania Danych Osobowych lub przyjęcia Danych Osobowych do dalszego przetwarzania od innego podmiotu przetwarzającego, Użytkownik, który taką informację poweźmie, zawiadamia o tym Koordynatora ds. ODO. 4.6.22 Koordynator ds. ODO rozstrzyga, czy dana sytuacja obejmuje dalsze powierzenie Danych Osobowych do przetwarzania i w takiej sytuacji zawiadamia MGGP S.A. lub osobę upoważnioną przez MGGP S.A. do decydowania o powierzeniu Danych Osobowych. 4.6.23 MGGP S.A, po zasięgnięciu opinii Koordynatora ds. ODO zobowiązany jest ocenić, czy z danym powierzeniem do dalszego przetwarzania lub przyjęciem Danych Osobowych do dalszego przetwarzania wiąże się obowiązek przeprowadzenia Oceny Skutków dla Ochrony Danych, stosując w tym celu metodykę szacowania ryzyka określoną w *Procedurze III.E.3 Zarządzanie ryzykiem dotyczącym bezpieczeństwa informacji i ochrony Danych Osobowych*. 4.6.24 Decyzję o powierzeniu lub przyjęciu Danych Osobowych do dalszego przetwarzania podejmuje MGGP S.A. lub upoważniona w tym zakresie osoba. 4.6.25 Dokonując wyboru podmiotu zewnętrznego, któremu powierzone mają zostać Dane Osobowe do dalszego przetwarzania, MGGP S.A. dokonuje weryfikacji, czy daje on wystarczające gwarancje wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom prawa, w tym w zakresie bezpieczeństwa przetwarzania, w szczególności jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby. 4.6.26 Powierzenie lub przyjęcie Danych Osobowych do dalszego powierzenia przetwarzania odbywa się na podstawie Umowy Podpowierzenia lub innego instrumentu zawierającego Klauzule dalszego powierzenia, zawartych na piśmie lub w formie elektronicznej pomiędzy MGGP S.A, a podmiotem trzecim, któremu zleca się czynności, związane z dalszym przetwarzaniem Danych Osobowych, lub który takie czynności zleca MGGP S.A. 4.6.27 W przypadku powierzenia danych do dalszego powierzenia przetwarzania wewnątrz krajów UE należy stosować *Umowę Podpowierzenia (Formularz III.E.1-F15)*. W przypadku dalszego powierzenia Danych do państw trzecich należy stosować klauzule opisane w *Formularzu III.E.1-F13*. 4.6.28 Koordynator ds. ODO odpowiada za zamieszczenie w Umowie Podpowierzenia lub wykorzystywanym instrumencie prawnym, informacji wymaganych zgodnie ze wzorem Umowy Podpowierzenia lub Klauzul Dalszego Powierzenia, w tym w szczególności wskazanie: przedmiotu i czasu trwania przetwarzania, charakteru i celu przetwarzania, rodzaju Danych Osobowych oraz kategorii osób, których Dane dotyczą, obowiązków i praw MGGP S.A. a także uregulowanie ewentualnego dopuszczenia korzystania z dalszych podmiotów przetwarzających Dane Osobowe w ramach tej umowy/instrumentu prawnego (wraz z podaniem ich pełnej nazwy, adresu i danych kontaktowych). 4.6.29 Projekt umowy dotyczącej dalszego powierzenia Danych Osobowych do przetwarzania podmiotowi trzeciemu lub przyjęcia Danych Osobowych od podmiotu trzeciego do dalszego przetwarzania, który nie został przygotowany zgodnie ze Wzorem Umowy Podpowiedzenia, wymaga każdorazowo akceptacji MGGP S.A., która poprzedzona winna być konsultacją z Koordynatorem ds. ODO i Działem Prawnym pod kątem zgodności z przepisami prawa powszechnie obowiązującego oraz niniejszą Polityką. 4.6.30 Podpisanie Umowy Podpowierzenia Danych Osobowych, Koordynator ds. ODO odnotowuje w *Rejestrze Umów Powierzenia (Formularz III.E.1-F2)*, który zawiera informacje o stronach takiej umowy. 4.6.31 Po zakończeniu trwania okresu przetwarzania Danych Osobowych powierzonych podmiotowi trzeciemu do dalszego przetwarzania Koordynator ds. ODO weryfikuje, czy podmiot ten zwrócił lub usunął Dane Osobowe, chyba że przepisy prawa, którym podlega podmiot przetwarzający, nakładają obowiązek przechowywania Danych Osobowych. 4.6.32 Dalsze przekazanie Danych do państwa trzeciego jest możliwe, jeżeli Komisja Europejska stwierdzi, że Państwo to zapewnia odpowiedni stopień ochrony (art. 45 RODO) lub jeżeli zastosowane zostaną odpowiednie zabezpieczenia, o których mowa w art. 46 RODO. Jeżeli przekazanie nie może się opierać na art. 45 ani 46 RODO, ADO weryfikuje, czy następuje jeden z wyjątków wskazanych w art. 49 RODO, a decydując się w takiej sytuacji na przekazanie, informuje osoby, których Dane dotyczą, o takim przekazaniu i o ważnych prawnie uzasadnionych interesach realizowanych przez ADO. W przypadku powierzenia Danych do państw trzecich należy podpisać z podmiotem przetwarzającym umowę, która powinna zawierać wszystkie klauzule opisane w *Formularzu III.E.1-F13*. Poza tym wymagane jest wypełnienie: Dodatku nr 1 – zawierającego m.in. opis podmiotów, kategorie Danych i czynności przetwarzania, Dodatku nr 2 – zawierającego opis środków bezpieczeństwa
Nr 4.7	**Rejestr czynności przetwarzania** 1.7.1. Administrator prowadzi *Rejestr czynności przetwarzania* według wzoru stanowiącego *Formularz III.E.1-F3*. W rejestrze tym zamieszcza się wszystkie następujące informacje: a) imię i nazwisko lub nazwę oraz dane kontaktowe ADO oraz wszystkich współadministratorów (przynajmniej dwóch administratorów wspólnie ustalających cele i sposoby przetwarzania), a także, gdy ma to zastosowanie – przedstawiciela ww. ADO oraz IOD, b) cele przetwarzania, c) opis kategorii osób, których Dane dotyczą, oraz kategorii Danych Osobowych, d) gdy ma to zastosowanie – odwołanie do zbiorów Danych Osobowych, e) kategorie odbiorców, którym Dane Osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,

	f) gdy ma to zastosowanie – przekazania Danych Osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a także dokumentację odpowiednich zabezpieczeń, jeżeli wymagane są przez RODO, g) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii Danych, h) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa. 1.7.2. W sytuacji przyjęcia do przetwarzania Danych Osobowych, organizacja prowadzi (jako podmiot przetwarzający) *Rejestr kategorii czynności przetwarzania (Formularz III.E.1-F12)*. W rejestrze tym zamieszcza się wszystkie następujące informacje: a) imię i nazwisko lub nazwę oraz dane kontaktowe podmiotu przetwarzającego oraz każdego administratora (w imieniu którego działa podmiot przetwarzający), a także gdy ma to zastosowanie – przedstawiciela administratora oraz IOD, b) kategorie przetwarzań dokonywanych w imieniu każdego administratora, c) gdy ma to zastosowanie, przekazania Danych Osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a także dokumentację odpowiednich zabezpieczeń, jeżeli wymagane są przez RODO, d) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.
Nr 4.8	**Wykonywanie obowiązków zgodnie z zasadą „privacy by design" oraz wykonywanie oceny skutków** 1.8.1. Ogólne założenia uwzględnienia ochrony Danych Osobowych w fazie projektowania (planowania). 1.8.1.1. Prowadząc działalność ADO rozpoznaje na bieżąco nowe sytuacje związane z przetwarzaniem Danych Osobowych oraz wdraża odpowiednie środki techniczne i organizacyjne, zaprojektowane w celu skutecznej realizacji zasad ochrony Danych oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi wynikające z przepisów oraz chronić prawa osób, których Dane dotyczą. ADO uwzględniać winien w tym zakresie w szczególności: a) stan wiedzy technicznej, b) koszt wdrażania, c) charakter, zakres, kontekst przetwarzania, d) cele przetwarzania, oraz e) ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikających z przetwarzania. 1.8.1.2. Wdrażając odpowiednie środki techniczne i organizacyjne, ADO zawsze dba, aby domyślnie przetwarzane były wyłącznie te Dane Osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych Danych Osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki wdrażane przez ADO zapewniają, by domyślnie Dane Osobowe nie były udostępniane bez interwencji PDO nieokreślonej liczbie osób fizycznych. 1.8.1.3. ADO każdorazowo rozpoznając nową sytuację przetwarzania lub decydując o wdrożeniu nowych środków zobowiązany jest stwierdzić czy zachodzi wysokie ryzyko naruszenia praw i wolności PDO. Wysokie ryzyko naruszenia praw i wolności PDO zachodzi podczas działań: a) przetwarzania Danych Osobowych mogącego prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, w szczególności jeżeli przetwarzanie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności Danych Osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną;, b) które utrudniają osobom, których Dane dotyczą, wykonywanie przysługujących im praw, c) które mogą powodować, że osoby, których Dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi Danymi Osobowymi, d) gdy podejmowanie decyzji wywołujących skutki prawne wobec osób ma następować w sposób zautomatyzowany, e) gdy podejmowanie decyzji wobec konkretnej osoby fizycznej ma następować po dokonaniu systematycznej, kompleksowej oceny czynników osobowych, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osób fizycznych na podstawie profilowania tych Danych, f) przetwarzania szczególnych kategorii danych, danych biometrycznych lub Danych Osobowych dotyczących wyroków skazujących, naruszeń prawa lub odnośnych środków bezpieczeństwa – za wyjątkiem, gdy przetwarzanie takie ma charakter incydentalny, g) w ramach których przetwarzanie dotyczy dużej ilości Danych Osobowych i wpływa na dużą liczbę osób, których Dane dotyczą, h) monitorowania na dużą skalę miejsc publicznie dostępnych, i) w ramach których Dane są przekazywane do państw trzecich, j) w ramach których przetwarzane są Dane Osobowe osób wymagających szczególnej opieki, w szczególności dzieci, k) polegających na połączeniu lub porównaniu dwóch lub większej ilości zbiorów Danych, l) w ramach których zachodzi innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych lub organizacyjnych, m) zamieszczonych w wykazie operacji przetwarzania wymagających Oceny Skutków opublikowanym przez Organ Nadzorczy lub przez inny właściwy organ władzy publicznej. 1.8.2. W sytuacji wątpliwości, czy spełniona jest którakolwiek z przesłanek wskazanych powyżej przyjąć należy, że ryzyko takie zachodzi. Identyfikacja nowej sytuacji przetwarzania Danych Osobowych. 1.8.2.1. Jeżeli Użytkownik stwierdzi, że Dane Osobowe są przetwarzane w odmienny sposób niż dotychczas, a w szczególności w oparciu o informacje zawarte w *Rejestrze Czynności Przetwarzania (Formularz III.E.1-F3)* stwierdzi, że: a) przetwarzane mają być Dane, których wcześniej nie przetwarzano, b) posiadane Dane są przetwarzane w nowym celu, c) Dane mają być przekazane do nowego podmiotu,

d) Dane mają być przetwarzane w nowy sposób wcześniej niepraktykowany (za pomocą nowych środków lub innymi metodami), albo
e) na skutek zmiany okoliczności przetwarzanie Danych w dotychczasowy sposób rodzić może nowe ryzyka,

to Użytkownik niezwłocznie zgłosi zaistniałą sytuację Koordynatorowi ds. ODO.

1.8.2.2. Zgłoszenie powinno zostać przekazane do Koordynatora ds. ODO bez zbędnej zwłoki.
1.8.2.3. Koordynator ds. ODO, po przeanalizowaniu otrzymanego zgłoszenia i potwierdzenia informacji w nim zawartych lub w sytuacji stwierdzenia zaistnienia ww. okoliczności, zawiadamia ADO o identyfikacji nowej sytuacji przetwarzania.
1.8.2.4. Jeżeli dojdzie do identyfikacji nowej sytuacji przetwarzania Danych, Koordynator ds. ODO przed rozpoczęciem przetwarzania (w razie potrzeby konsultując się z Zespołem ds. ODO) przedstawia swoją rekomendację ADO, który decyduje czy konieczne jest przeprowadzenie Oceny Skutków.
1.8.2.5. W przypadku, gdy nowa sytuacja przetwarzania tego wymaga, Koordynator ds. ODO dokona stosownej aktualizacji w *Rejestrze czynności przetwarzania (Formularz III.E.1-F3)* oraz w innych dokumentach, a także zawiadomi o tym ADO.

1.8.3. Identyfikacja nowego systemu informatycznego.
1.8.3.1. Użytkownik każdorazowo zawiadamia ASI oraz Koordynatora ds. ODO o zamiarze wykorzystania nowego systemu informatycznego służącego przetwarzaniu Danych Osobowych.
1.8.3.2. Po otrzymaniu zawiadomienia, o którym mowa w punkcie powyższym, lub po uzyskaniu z jakiegokolwiek innego źródła wiedzy o nowym systemie informatycznym, Koordynator ds. ODO potwierdza czy dany system będzie służył do przetwarzania Danych Osobowych i czy będą miały do niego zastosowanie odpowiednie przepisy ochrony Danych Osobowych.
1.8.3.3. W przypadku stwierdzenia, że nowy system informatyczny ma służyć przetwarzaniu Danych Osobowych, Koordynator przeprowadza ocenę systemu informatycznego zgodnie z kwestionariuszem zawartym w *Raporcie z oceny systemu informatycznego (Formularz III.E.1-F10).*
1.8.3.4. W ramach oceny Koordynator ds. ODO zwraca się do dostawcy nowego systemu informatycznego o przekazanie informacji o przeprowadzeniu przez tego dostawcę lub producenta Oceny Skutków, a także o wynikach tej Oceny Skutków.
1.8.3.5. Przed rozpoczęciem przetwarzania Danych z wykorzystaniem nowego systemu informatycznego Koordynator ds. ODO (po konsultacji z Zespołem ds. ODO) przedstawia swoją rekomendację ADO, który decyduje również, czy konieczne jest przeprowadzenie Oceny Skutków.
1.8.3.6. Wyniki Oceny wraz z rekomendacją co do wdrożenia nowego Systemu Koordynator ds. ODO przedstawia ADO.

1.8.4. Otrzymanie danych do przetwarzania od innych podmiotów.
1.8.4.1. Jeżeli Użytkownik, przed przystąpieniem lub w trakcie Przetwarzania Danych stwierdzi, że Dane otrzymane do Przetwarzania od innego podmiotu niż PDO stanowią Dane Osobowe, zgłosi zaistniałą sytuację do Koordynatora ds. ODO.
1.8.4.2. Zgłoszenie powinno zostać przekazane Koordynatorowi ds. ODO bez względnej zwłoki.
1.8.4.3. ADO lub wskazany przez niego Koordynator ds. ODO zwraca się do podmiotu przekazującego Dane Osobowe o przekazanie informacji o przeprowadzeniu przez ten podmiot Oceny skutków, a także o wynikach tej Oceny Skutków.
1.8.4.4. Koordynator ds. ODO weryfikuje, czy konieczne jest podpisanie Umowy Powierzenia, a także podejmuje kroki, o których mowa w punkcie 4.6 niniejszej Polityki.
1.8.4.5. Koordynator ds. ODO, po przeanalizowaniu zgłoszenia oraz po wykonaniu czynności wskazanych w powyższych punktach, podejmuje decyzję czy w danej sytuacji dochodzi do otrzymania do Przetwarzania od innych podmiotów Danych Osobowych, a także każdorazowo przedstawia swoją rekomendację ADO, który podejmuje decyzję, czy należy przeprowadzić Ocenę skutków, zawiadamiając niezwłocznie Zarząd ADO.

1.8.5. Zasady przeprowadzania Oceny skutków.
1.8.5.1. Ocena Skutków jest szczególnie wymagana w przypadkach wskazanych w punkcie 4.8.1.3.
1.8.5.2. Od Użytkownika, który zidentyfikował sytuację przetwarzania, z którą związana jest Ocena Skutków, należy uzyskać wszystkie informacje, jakimi dysponuje on w zakresie potrzebnym na cele wykonania Oceny Skutków.
1.8.5.3. Z przeprowadzonej Oceny Skutków sporządza się *Sprawozdanie z oceny skutków przetwarzania danych (Formularz III.E.1-F11).* Ocena Skutków zawiera co najmniej:

a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez ADO, składający się z:
   - charakteru, zakresu, kontekstu i celów przetwarzania,
   - udokumentowanych Danych Osobowych, odbiorców oraz okresu przechowywania Danych Osobowych,
   - funkcjonalnego opisu operacji przetwarzania,
   - aktywów, na których opierają się Dane Osobowe (np. sprzęt, oprogramowanie, sieci, ludzie, dokumenty papierowe lub papierowe kanały transmisji),
   - zgodności z zatwierdzonymi kodeksami postępowania;
b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów, w ramach której ocenia się:
   - środki wpływające na niezbędność i proporcjonalność przetwarzania oceniając:
     - ✓ konkretny, wyraźny i prawnie uzasadniony cel przetwarzania,
     - ✓ zgodność przetwarzania z prawem,
     - ✓ czy środki są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów przetwarzania,
     - ✓ ograniczenie okresu przechowywania Danych;
   - środki przyczyniające się do praw osób, których Dane dotyczą oceniając:
     - ✓ czy prawidłowo udzielane są osobie, której Dane dotyczą odpowiednie informacje,
     - ✓ czy zapewniono prawo dostępu i przekazywania Danych,
     - ✓ czy zapewniono prawo do sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu,
     - ✓ jacy występują odbiorcy Danych,

	✓ jakie występują podmioty przetwarzające, ✓ jakie są planowane zabezpieczenia dotyczące przekazywania Danych, ✓ czy wymagane są uprzednie konsultacje; c) ocenę ryzyka naruszenia praw lub wolności osób, których Dane dotyczą, oceniając: • źródło, charakter, specyfikę i powagę każdego ryzyka (nieuprawnionego dostępu, niepożądanej modyfikacji i zniknięcia danych) z punktu widzenia osób, których Dane dotyczą, • potencjalne skutki dla praw lub wolności osób, których Dane dotyczą, identyfikowane w przypadku nieuprawnionego dostępu, niepożądanej modyfikacji i zniknięcia danych, • zagrożenia, które mogłyby prowadzić do nieuprawnionego dostępu, niepożądanej modyfikacji i zniknięcia Danych, • oszacowanie prawdopodobieństwa i powagi tego ryzyka; d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę Danych Osobowych i wykazać przestrzeganie przepisów i niniejszej Procedury, z uwzględnieniem praw i prawnie uzasadnionych interesów PDO i innych osób, których sprawa dotyczy. 1.8.5.4. W stosownych przypadkach Koordynator ds. ODO decyduje, czy należy zasięgać w trakcie dokonywania Oceny Skutków opinii osób, których Dane dotyczą, lub ich przedstawicieli w sprawie zamierzonego przetwarzania. Zasięgnięcie opinii nie może powodować uszczerbku dla ochrony interesów handlowych ADO lub interesów publicznych lub bezpieczeństwa operacji przetwarzania. 1.8.5.5. W przypadku dokonywania Oceny Skutków dla istniejącej już sytuacji przetwarzania, w które zaangażowany jest Procesor lub dla nowej sytuacji przetwarzania, dla której zaangażowany ma być określony, znany już Procesor, Koordynator ds. ODO zobowiązany jest zaangażować Procesora w Ocenę Skutków, uzyskując od Procesora informacje niezbędne w zakresie, w jakim Dane będzie przetwarzał Procesor. 1.8.5.6. Jeżeli Ocena Skutków wskaże, że przetwarzanie Danych Osobowych objętych Oceną Skutków powodowałoby wysokie ryzyko, gdyby nie zastosowano środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania Koordynator ds. ODO informuje Zarząd ADO o konieczności konsultacji się z Organem Nadzorczym, a następnie ADO dokonuje takich konsultacji. W przypadku stwierdzenia wymogu konsultacji z Organem Nadzorczym, po zakończeniu prowadzenia Oceny Skutków Koordynator ds. ODO, po uzyskaniu stanowiska Zarządu przekazuje Organowi Nadzorczemu również sprawozdanie z przeprowadzenia tej Oceny. 1.8.5.7. Użytkownicy w miarę możliwości technicznych są informowani o decyzji oraz wynikach Oceny Skutków. 1.8.5.8. Koordynator ds. ODO podejmuje czynności w celu uaktualnienia Procedur i Rejestru czynności przetwarzania w związku z nową sytuacją przetwarzania Danych Osobowych oraz wynikami Oceny Skutków. 1.8.5.9. Dla podobnych operacji przetwarzania Danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić wspólną Ocenę Skutków lub zastosować Ocenę Skutków, która już była przeprowadzona wcześniej, o czym każdorazowo decyduje ADO na podstawie rekomendacji udzielonej przez Koordynatora ds. ODO. 1.8.5.10. Wyniki przeprowadzonej Oceny Skutków powinny być brane pod uwagę przy dokonywaniu przez Koordynatora ds. ODO okresowego szacowania ryzyka. W szczególności w przypadku stwierdzenia zmiany ryzyka związanego z operacją przetwarzania, która poddana była Ocenie Skutków Koordynator ds. ODO po zasięgnięciu opinii Zespołu ds. ODO może zdecydować o powtórzeniu Oceny Skutków, o wynikach której niezwłocznie poinformuje ADO. 1.8.5.11. ADO może zrezygnować z przeprowadzenia Oceny Skutków, jeżeli nowa sytuacja przetwarzania polega na przetwarzaniu Danych Osobowych, które: a) jest niezbędne do wypełnienia obowiązku prawnego ciążącego na ADO, lub b) jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej ADO a także każdorazowo, c) ma podstawę prawną w przepisach regulujących daną operację przetwarzania lub zestaw operacji, a Oceny Skutków dla ochrony Danych dokonano w ramach procesu legislacyjnego, a przepisy nie nałożyły wyraźnie obowiązku przeprowadzenia Oceny Skutków. 1.8.5.12. Koordynator ds. ODO jest zobowiązany do prowadzenia dokumentacji podjętych przez ADO czynności i decyzji w zakresie Oceny Skutków, w szczególności powinien dokumentować rezygnację z przeprowadzenia Oceny Skutków i podstawy takiej rezygnacji, a także przechowywać *Sprawozdania z oceny skutków przetwarzania danych (Formularz III.E.1-F11)*. 1.8.5.13. Wyniki przeprowadzonej Oceny Skutków winny znaleźć odzwierciedlenie w treści Umowy Powierzenia, jeżeli w proces przetwarzania objęty Oceną Skutków zaangażowany ma być Procesor.
Nr 4.9	**Plan sprawdzeń oraz dokonywanie sprawdzeń** 4.9.1. ADO zapewnia zastosowanie zabezpieczeń niezbędnych dla zapewnienia praw i wolności osób, których Dane dotyczą, z uwzględnieniem charakteru, zakresu i celów przetwarzania oraz kategorii przetwarzania. 4.9.2. W związku z powyższym Koordynator ds. ODO przeprowadza okresowe szacowanie ryzyka zagrożeń dla zbiorów danych i monitorowanie zastosowanych zabezpieczeń. W ramach okresowego szacowania ryzyka wykonana zostanie co najmniej jedna kontrola wewnętrzna w każdym roku kalendarzowym. Możliwe jest przeprowadzenie w danym roku kontroli wewnętrznej dla wybranego zbioru Danych lub procesu przetwarzania osobno lub dla grup zbiorów Danych lub procesów. 4.9.3. Przeprowadzenie kontroli wewnętrznej potwierdzone zostanie sporządzeniem i podpisaniem *Protokołu z kontroli wewnętrznej ODO (Formularz III.E.1-F9).* 4.9.4. W stosunku do operacji przetwarzania, które ze względu na swój charakter, zakres, kontekst i cele mogą powodować wysokie ryzyko naruszenia praw i wolności osób trzecich, czynności sprawdzające przeprowadza się co najmniej raz na pół roku. W szczególności dotyczy to operacji: a) przetwarzania Danych Osobowych mogącego prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, w szczególności jeżeli przetwarzanie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną,

	b) które utrudniają osobom, których Dane dotyczą, wykonywanie przysługujących im praw, c) które mogą powodować, że osoby, których Dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi Danymi Osobowymi, d) podejmowanych w celu podjęcia decyzji wobec konkretnej osoby fizycznej po dokonaniu systematycznej, kompleksowej oceny czynników osobowych, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osób fizycznych na podstawie profilowania tych Danych, e) przetwarzania szczególnych kategorii Danych, danych biometrycznych lub Danych Osobowych dotyczących wyroków skazujących, naruszeń prawa lub odnośnych środków bezpieczeństwa, f) w ramach których przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których Dane dotyczą, g) monitorowania na dużą skalę miejsc publicznie dostępnych, h) w ramach których Dane są przekazywane do państw trzecich, i) jeżeli przetwarzane są Dane Osobowe osób wymagających szczególnej opieki, w szczególności dzieci. 4.9.5. Po przeprowadzeniu kontroli i sporządzeniu *Protokołu z kontroli wewnętrznej ODO (Formularz III.E.1-F9)* Koordynator ds. ODO powiadamia ADO o wynikach kontroli oraz o ewentualnych wskazaniach co do zmian istniejących Procedur oraz zabezpieczeń. 4.9.6. ADO, po konsultacjach z Zespołem ds. ODO, podejmuje decyzję w sprawie proponowanych przez Koordynatora ds. ODO rozwiązań problemów, których występowanie stwierdzono podczas kontroli wewnętrznej. 4.9.7. Koordynator ds. ODO w trakcie kolejnej kontroli wewnętrznej dokona sprawdzenia wdrożenia i funkcjonowania środków wprowadzonych w następstwie poprzedniej kontroli. 4.9.8. Koordynator ds. ODO prowadzi rejestr przeprowadzonych kontroli wewnętrznych, w którym odnotowuje: termin wykonania kontroli, zakres wykonanej kontroli, problemy stwierdzone w trakcie kontroli oraz informację o zaproponowanych/wdrożonych rozwiązaniach.
Nr 4.10	**Osoby upoważnione do przetwarzania Danych Osobowych** 4.10.1. Każda osoba, która ma być dopuszczona do przetwarzania Danych, musi posiadać odpowiednie upoważnienie do przetwarzania Danych, nadane przez ADO 4.10.2. Upoważnienie powinno zawierać co najmniej: a) datę z którą zostało nadane; b) datę z którą upoważnienie wygasa jeżeli jest ono nadane na czas określony; c) zakres upoważnienia. 4.10.3. Upoważnienie do przetwarzania Danych Osobowych wygasa z chwilą: ustania zatrudnienia Użytkownika u ADO lub współpracy z ADO w oparciu o inną podstawę prawną lub w przypadku, gdy zostało nadane na czas określony z upływem czasu na jaki zostało nadane. Przełożony lub Opiekun Użytkownika jest obowiązany niezwłocznie poinformować ADO/Koordynatora ds. ODO o ustaniu zatrudnienia/współpracy z Użytkownikiem. Upoważnienie wygasa także w przypadku jego odwołania przez ADO. 4.10.4. Osoba upoważniona przez ADO nie ma prawa do udzielania dalszych upoważnień, chyba że upoważnienie do przetwarzania Danych Osobowych nadane przez ADO zawiera upoważnienie do udzielania dalszych upoważnień. 4.10.5. Wzór upoważnień do przetwarzania danych stanowią *Formularz III.E.1-F4a, Formularz III.E.1-F4b i Formularz III.E.1-F4c.* 4.10.6. ADO lub upoważniona do tego osoba nadając Użytkownikowi upoważnienia do przetwarzania Danych Osobowych zobowiązana jest poinformować Użytkownika o obowiązku zapoznania się z przepisami o ochronie Danych Osobowych, Procedurami oraz umożliwić dostęp do tych przepisów i Procedur w odpowiednim zakresie. 4.10.7. Koordynator ds. ODO zobowiązany jest prowadzić regularne ocenianie i weryfikowanie praw dostępu Użytkowników. 4.10.8. Udzielone upoważnienie może być w każdym czasie cofnięte/zmienione/ograniczone. 4.10.9. W uzasadnionych przypadkach przełożony Użytkownika lub Opiekun zobowiązani są niezwłocznie zawnioskować o cofnięcie, ograniczenie lub inną modyfikację zakresu upoważnienia Użytkownika do przetwarzania Danych mogącą w szczególności wynikać z: a) zmiany zakresu obowiązków służbowych Użytkownika; b) spowodowania incydentu, który skutkował Naruszeniem ODO lub miał inny negatywny wpływ na bezpieczeństwo przetwarzania Danych Osobowych; c) naruszenia niniejszych Procedur lub przepisów regulujących przetwarzanie Danych Osobowych.
Nr 4.11	**Ewidencja zbiorów i osób upoważnionych** 4.11.1. ADO obowiązany jest do prowadzenia *Ewidencji zbiorów i osób upoważnionych (Formularz III.E.1-F5).* 4.11.2. Ewidencja może być prowadzona w wersji papierowej lub elektronicznej z możliwością jej wydruku. 4.11.3. Ewidencja zawiera: a) szczegółowe informacje na temat zbiorów Danych Osobowych, b) imię i nazwisko osoby upoważnionej, c) datę nadania i ustania oraz zakres upoważnienia do przetwarzania Danych Osobowych.
Nr 4.12	**Postępowanie w razie zgłoszenia przez PDO żądania skorzystania z uprawnień** 4.12.1. Ogólne obowiązki w razie przyjęcia żądania. 4.12.1.1. PDO może zgłosić zarówno do Danych, których ADO jest administratorem, jak i do tych, które ADO przetwarza na zlecenie osoby trzeciej, żądanie wykonania obowiązków w zakresie: a) prawa do otrzymania informacji o operacjach przetwarzania b) prawa do otrzymania kopii Danych Osobowych, c) prawa do przenoszenia Danych Osobowych, d) prawa do usunięcia Danych („prawa do bycia zapomnianym"), e) prawa do ograniczenia przetwarzania Danych Osobowych, f) prawa do sprostowania lub uzupełnienia Danych, g) prawa do sprzeciwu wobec przetwarzania Danych Osobowych, h) prawa do niepodlegania decyzji opierającej się wyłącznie na zautomatyzowanym przetwarzaniu.

4.12.1.2. W przypadku otrzymania żądania skorzystania z Uprawnień PDO każdy Użytkownik, zobowiązany jest:
- a) w przypadku otrzymania żądania w formie innej niż pisemna, mailowa lub elektroniczna (za pomocą narzędzia udostępnianego przez ADO), w szczególności w przypadku otrzymania takiego żądania w formie ustnej lub telefonicznie – poinformować o możliwości złożenia żądania w formie pisemnej, mailowej lub za pomocą narzędzia udostępnianego przez ADO,
- b) w przypadku, gdy PDO sam nie poda takich informacji w treści żądania, niezwłocznie wezwać osobę dokonującą żądania do uzupełnienia żądania o podanie danych pozwalających na zidentyfikowanie tej osoby co najmniej poprzez podanie:
  - imienia i nazwiska DPO, stosunku łączącego PDO z ADO (np. aktualny, potencjalny, lub były pracownik, współpracownik ADO, pracownik, współpracownik podmiotu powiązanego z ADO, klient ADO, adresat marketingu bezpośredniego ADO),
  - dodatkowej informacji dostatecznie identyfikującej osobę składającą żądanie, która to cecha nie może być informacją powszechnie dostępną (jak np. numer NIP przedsiębiorcy), i jednocześnie powinna być znana lub możliwa do identyfikacji przez ADO (np. numeru PESEL, serii i numeru dokumentu tożsamości, danych dostępowych do systemu informatycznego ADO, do którego dostęp ma PDO),
  - co najmniej jednej informacji dotyczącej zakresu Danych tej osoby, jakie przetwarza ADO,
  - w przypadku dalszych wątpliwości co do tożsamości, należy żądać przesłania dodatkowych informacji potwierdzających tożsamość PDO, lub przesłania żądania w formie pisemnej na adres korespondencyjny ADO.
- c) odnotować w formie protokołu otrzymanie żądania wykonania określonego Uprawnienia PDO wykorzystując w tym celu formularz *Protokół przyjęcia i realizacji żądania PDO (Formularz III.E.1-F6)*, oraz
- d) niezwłocznie, nie później niż w ciągu 2 godzin, przekazać kopię takiego protokołu do Koordynatora ds. ODO przesyłając drogą mailową lub za pomocą innego narzędzia wewnętrznej komunikacji powszechnie wykorzystywanego u ADO i pozwalającego na odnotowanie zgłoszenia, a także powiadomić bezpośredniego przełożonego w strukturze organizacyjnej ADO o zgłoszeniu żądania.

4.12.1.3. Protokół, o którym stanowi punkt powyżej zawierać powinien:
- a) dane dostatecznie identyfikujące osobę, która wystosowała żądanie, wraz z informacją, jeżeli Użytkownik wystąpił o dodatkowe dane identyfikujące składającego żądanie,
- b) informację o tym, czy osoba, która wystosowała żądanie jest osobą, której Dane dotyczą,
- c) treść żądania,
- d) datę i godzinę doręczenia żądania,
- e) formę w jakiej dostarczono żądanie,
- f) informację czy żądanie związane jest z ewentualnym podejrzeniem Naruszenia ODO - należy się upewnić, czy wdrożono wszelkie odpowiednie techniczne środki ochrony i wszelkie odpowiednie środki organizacyjne, by od razu stwierdzić naruszenie ochrony Danych Osobowych,
- g) imię, nazwisko i identyfikator Użytkownika, który przyjął żądanie.

4.12.2. Czynności podejmowane w odpowiedzi na żądanie osoby, której Dane dotyczą:

4.12.2.1. Niezwłocznie po otrzymaniu zawiadomienia od Użytkownika, Koordynator ds. ODO zobowiązany jest podjąć następujące działania:
- a) ponownie ocenić, czy żądanie pochodzi od osoby, której dane dotyczą, w razie potrzeby zażądać odpowiednich informacji zgodnie z punktem 4.12.1.2 powyżej, a także ocenić, czy ADO przetwarza Dane Osobowe tej osoby, zwracając się w tym celu w razie potrzeby do właścicieli poszczególnych zbiorów Danych,
- b) zweryfikować spełnienie odpowiednich przesłanek dla skorzystania z uprawnienia PDO, którego żądanie dotyczy (przesłanki zdefiniowane w *Protokole przyjęcia i realizacji żądania PDO - Formularz III.E.1-F6)*,
- c) w przypadku pozytywnej weryfikacji tożsamości uprawnionego podmiotu oraz przesłanek do skorzystania z uprawnienia PDO – odnieść się do żądania zgodnie z punktami poniższymi.

4.12.2.2. Koordynator ds. ODO ocenia zasadność wniosku, w tym zakresie istnienia powodu odmowy dostępu do Danych, a w szczególności ocenia:
- a) czy ADO jest uprawniony do odmowy uczynienia zadość żądaniu,
- b) czy ustawowe ograniczenia, o których mowa w art. 23 RODO, nie zezwalają na dostęp w ramach określonych w nim warunków wstępnych,
- c) czy przekazanie kopii Danych Osobowych naruszałoby prawa innych osób,
- d) czy wniosek o dostęp jest oczywiście bezpodstawny z uwagi na skierowanie żądania do niewłaściwego podmiotu.

4.12.2.3. W przypadku, gdy żądanie jest zasadne Koordynator ds. ODO wykonuje go zgodnie z jego treścią. Jeżeli wykonanie żądania tego wymaga, Koordynator ds. ODO:
- a) dokonuje stosownych zmian w *Rejestrze Czynności przetwarzania (Formularz III.E.1-F3)*,
- b) zwraca się do właścicieli poszczególnych zbiorów Danych oraz do procesorów przetwarzających Dane dotyczące PDO zgłaszającego żądanie, o niezbędną pomoc w wykonaniu tego żądania.

4.12.2.4. W przypadku wystąpienia podstaw do odmowy wykonania żądania PDO, Koordynator ds. ODO zawiadomi o tym PDO, informując o powodach odmowy oraz o możliwości wniesienia skargi do Organu Nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

4.12.2.5. W razie potrzeby, w tym wystąpienia niejasności w związku z żądaniem, należy skorzystać z pomocy Zespołu ds. ODO.

4.12.2.6. Koordynator ds. ODO zobowiązany jest udokumentować okoliczności i przebieg czynności podjętych wskutek wniesionego żądania, według wzoru stanowiącego *Protokół przyjęcia i realizacji żądania PDO (Formularz III.E.1-F6).*

4.12.2.7. Jeżeli treść żądania lub okoliczności wskazują na faktyczne lub potencjalne Naruszenia ODO lub uzasadnione podejrzenie Naruszenia ODO, Koordynator ds. ODO jest odpowiedzialny za odnotowanie tego w *Rejestrze Naruszeń ODO (Formularz III.E.1-F8)* oraz natychmiastowe podjęcie czynności zgodnych z odpowiednią Procedurą.

4.12.2.8. Koordynator ds. ODO może uzależnić wykonanie żądania PDO od pokrycia kosztów jego wykonania, jeżeli żądanie jest ewidentnie nieuzasadnione lub nadmierne. W przypadku, gdy PDO wystąpi z żądaniem wykonania tego samego uprawnienia drugi raz w ciągu sześciu miesięcy Koordynator ds. ODO dokona oceny czy zdanie pierwsze znajdzie zastosowanie i poinformuje o tym niezwłocznie PDO, wskazując wysokość kosztów do uiszczenia, dane do przelewu oraz informując, że w przypadku braku zapłaty w terminie 7 dni ADO uprawniony będzie do odmowy wykonania żądania.

4.12.2.9. Wykonanie obowiązków ADO w odpowiedzi na żądanie PDO (uwzględnienie lub odmowa spełnienia żądania) nastąpi w terminie nie dłuższym niż jeden miesiąc od otrzymania żądania. Jeżeli zachowanie tego terminu z uwagi na skomplikowany charakter żądania lub ilość żądań nie jest możliwe, Koordynator ds. ODO może przedłużyć termin o kolejne dwa miesiące powiadamiając o tym PDO niezwłocznie, w terminie miesiąca od otrzymania żądania, wskazując przyczyny opóźnienia.

4.12.3. Obowiązki ADO w przypadku żądania w zakresie prawa do otrzymania informacji o operacjach przetwarzania oraz prawa do otrzymania kopii Danych Osobowych.

4.12.3.1. ADO uwzględnia, z zastrzeżeniem pkt. 4.12.3.4, żądanie PDO obejmujące:

a) potwierdzenie, czy ADO przetwarza Dane Osobowe dotyczące PDO,
b) udzielenie dostępu do Danych Osobowych PDO przetwarzanych przez ADO, w tym dostarczenia kopii tych Danych,
c) udzielenia informacji w zakresie Danych Osobowych PDO obejmujących:
- cel przetwarzania,
- kategorie przetwarzanych Danych Osobowych,
- konkretnych odbiorców lub kategorie odbiorców Danych Osobowych, w tym informacje, którzy z nich ulokowani są w państwach trzecich lub stanowią organizacje międzynarodowe,
- okres przechowywania Danych lub kryteria ustalenia tego okresu,
- prawo do żądania sprostowania lub usunięcia Danych dotyczących PDO, ograniczenia ich przetwarzania oraz wniesienia sprzeciwu wobec ich przetwarzania,
- prawo do wniesienia skargi do Organu Nadzorczego,
- źródło pochodzenia Danych, jeżeli nie zostały zebrane od PDO,
- informacje o zautomatyzowanym podejmowaniu decyzji wobec PDO, w tym profilowaniu oraz zasadach podejmowania tych decyzji i konsekwencjach takiego przetwarzania dla PDO.

4.12.3.2. Koordynator ds. ODO zwraca się do właścicieli poszczególnych zbiorów Danych oraz do Procesorów o zebranie Danych dotyczących PDO zgłaszającego żądanie i mieszczących się w zakresie wskazanym w punkcie powyżej.

4.12.3.3. W przypadku, gdy PDO złoży żądanie drogą elektroniczną ADO również doręcza kopię Danych Osobowych drogą elektroniczną, chyba że PDO w swoim żądaniu wyraźnie wskaże inaczej. ADO przesyła plik z zebranymi Danymi do PDO, który wystąpił z żądaniem w formie zaszyfrowanej. Klucz do odszyfrowania pliku przesyłany jest w osobnej wiadomości.

4.12.3.4. ADO może zdecydować o ograniczeniu przekazywanych informacji lub kopii Danych, jeżeli przekazanie ich w zakresie wskazanym przez PDO może negatywnie wpływać na prawa lub wolności innych osób, w tym tajemnice handlowe lub własność intelektualną, w szczególności na prawa autorskie.

4.12.4. Obowiązki ADO w przypadku żądania w zakresie prawa do przenoszenia Danych Osobowych.

4.12.4.1. ADO uwzględnia żądanie PDO i nakazuje przeniesienie Danych w sytuacjach, gdy spełnione są łącznie następujące przesłanki:

a) Dane przetwarzane są na podstawie zgody PDO lub w celu wykonania umowy, której PDO jest stroną,
b) Przetwarzanie odbywa się w sposób zautomatyzowany. W przypadku Danych przetwarzanych wyłącznie w formie papierowej Uprawnienie do przekazania Danych nie przysługuje,
c) Żądanie dotyczy Danych dostarczonych przez PDO, który zgłasza żądanie, co obejmuje:
- Dane aktywnie przekazane przez PDO lub
- Dane wynikające z obserwacji zachowania PDO lub wygenerowane w związku z tym zachowaniem (z wyłączeniem danych uzyskanych na skutek dokonywania przez ADO na tych Danych innych operacji, w tym danych wywnioskowanych i wywiedzionych z Danych PDO np. wyników analizy, działania algorytmów lub profilowania).

4.12.4.2. Koordynator ds. ODO zwraca się do właścicieli poszczególnych zbiorów Danych oraz do Procesorów o zebranie Danych dotyczących PDO zgłaszającego żądanie. Zebranie nastąpi w pliku w powszechnie używanym formacie nadającym się do odczytu maszynowego. Koordynator ds. ODO wyznacza rozsądny termin na zebranie Danych, wynoszący nie więcej niż dwa tygodnie, a także wzywa właścicieli zbiorów Danych oraz Procesorów, by w przypadku braku możliwości realizacji tego obowiązku niezwłocznie poinformowali o tym Koordynatora ds. ODO.

4.12.4.3. Koordynator ds. ODO zobowiązany jest zweryfikować czy w przekazywanych Danych zostały zawarte informacje o innych osobach fizycznych, które pozwalają na zidentyfikowanie tych osób (np. dane o osobach, z którymi PDO wchodził w interakcje). W takiej sytuacji Koordynator ds. ODO zawiadamia PDO o stwierdzeniu występowania takich danych i zwraca się do PDO, by ten złożył oświadczenie, czy Dane takich osób trzecich mają zostać przekazane razem z Danymi PDO. Koordynator ds. ODO odnotowuje złożenie oświadczenia oraz jego treść, datę i godzinę złożenia. W przypadku braku złożenia takiego oświadczenia przez PDO w terminie 7 dni, Koordynator ds. ODO w ramach technicznych możliwości dostępnych ADO, przekazuje dane takich osób trzecich w formie zanonimizowanej, lub odmawia wykonania żądania PDO.

4.12.4.4. ADO może zdecydować o ograniczeniu przekazywanych informacji, jeżeli przekazanie ich w zakresie wskazanym przez PDO może negatywnie wpływać na prawa lub wolności innych osób, w tym tajemnice handlowe lub własność intelektualną, w szczególności na prawa autorskie.

4.12.4.5. Koordynator ds. ODO przesyła plik z zebranymi Danymi do PDO, który wystąpił z żądaniem lub do osoby trzeciej wskazanej przez PDO. Plik z Danymi przesyłany jest w formie zaszyfrowanej. Klucz do odszyfrowania pliku przesyłany jest w osobnej wiadomości.

4.12.5. Obowiązki ADO w przypadku żądania w zakresie prawa do usunięcia Danych („prawa do bycia zapomnianym").

4.12.5.1. ADO zobowiązany jest uwzględnić żądanie PDO i dokonać usunięcia Danych w sytuacjach, gdy zachodzi jedna z poniższych okoliczności:
- a) Dane nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
- b) przetwarzanie odbywa się na podstawie zgody PDO, a PDO zgodę tą wycofa i ADO nie ma innej podstawy prawnej do przetwarzania;
- c) PDO wniósł sprzeciw wobec przetwarzania:
  - niezbędnego do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej,
  - niezbędnego do celów wynikających z prawnie uzasadnionych interesów realizowanych przez ADO lub osobę trzecią,
  - a nie istnieje nadrzędna prawnie uzasadniona podstawa przetwarzania;
- d) PDO wniósł sprzeciw wobec przetwarzania Danych, które przetwarzane były na potrzeby marketingu bezpośredniego,
- e) ADO przetwarzał Dane niezgodnie z prawem,
- f) obowiązek usunięcia Danych przez ADO wynika z obowiązującego przepisu prawa,
- g) dane PDO zebrano w celu świadczenia usług na jego rzecz, a w chwili zebrania jego Danych nie miał skończonych 18 lat.

4.12.5.2. Koordynator ds. ODO zwraca się do właścicieli poszczególnych zbiorów Danych oraz do procesorów o zidentyfikowanie wszystkich Danych dotyczących PDO zgłaszającego żądanie i mieszczących się w zakresie wskazanym w żądaniu i przekazanie Koordynatorowi ds. ODO zebranej informacji obejmującej kategorie Danych, zakres czynności przetwarzania, zbiory i systemy, w których pojawiają się te Dane. Koordynator ds. ODO wyznacza rozsądny termin na zebranie Danych, wynoszący nie więcej niż dwa tygodnie.

4.12.5.3. Koordynator ds. ODO każdorazowo występując o informację, o której mowa w punkcie powyżej zobowiązuje osoby tam wskazane do dokonania oceny, czy zachodzi jedna z przesłanek wskazanych w punkcie poniżej.

4.12.5.4. ADO może odmówić usunięcia danych w sytuacji, gdy przetwarzanie Danych PDO jest niezbędne:
- a) do ustalenia, dochodzenia lub ochrony roszczeń,
- b) do korzystania z prawa do wolności wypowiedzi i informacji,
- c) do wywiązania się z obowiązków prawnych ciążących na ADO,
- d) do wykonania zadania realizowanego w celu publicznym lub w ramach sprawowania władzy publicznej powierzonej ADO,
- e) z uwagi na interes publiczny w dziedzinie zdrowia publicznego,
- f) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych, do celów statystycznych.

4.12.5.5. Niezwłocznie po uzyskaniu informacji, o której mowa w punktach 4.12.5.2 i 4.12.5.3, Koordynator ds. ODO, w razie potrzeby po uprzedniej konsultacji z Zespołem ds. ODO, rekomenduje ADO sposób postępowania (czy należy dokonać usunięcia tych Danych). W przypadku podjęcia przez ADO decyzji o usunięciu, Koordynator ds. ODO przekazuje tą decyzję właścicielom zbiorów i procesorom, którzy po jej wykonaniu niezwłocznie przekażą IOD potwierdzenie usunięcia wraz ze wskazaniem jakie kategorie Danych, w jakich zbiorach i systemach zostały usunięte.

4.12.5.6. Usunięcie Danych obejmuje trwałe usunięcie poprzez ich skasowanie lub nadpisanie w sposób uniemożliwiający przywrócenie Danych, lub też ich anonimizację.

4.12.5.7. W przypadku upublicznienia Danych objętych żądaniem usunięcia (w szczególności na stronie internetowej ADO, w portalu społecznościowym), jeżeli ADO podejmie decyzję o usunięciu, ADO zobowiązany jest podjąć działania w celu poinformowania wszystkich administratorów, co do których ADO wie lub racjonalnie może zakładać, że przetwarzają te Dane (w szczególności administratora portalu społecznościowego), o żądaniu PDO ich usunięcia wraz z łączami do nich, ich kopiami oraz replikacjami.

4.12.6. Obowiązki ADO w przypadku żądania w zakresie prawa do ograniczenia przetwarzania Danych Osobowych.

4.12.6.1. ADO uwzględnia żądanie PDO i nakazuje ograniczenie przetwarzania Danych w sytuacjach, gdy:
- a) PDO kwestionuje prawidłowość Danych – do czasu zweryfikowania prawidłowości Danych przez ADO,
- b) Przetwarzanie jest niezgodne z prawem, jednak PDO sprzeciwi się usunięciu Danych przez ADO, żądając w zamian ograniczenia przetwarzania Danych,
- c) ADO utracił cele dla przetwarzania danych, ale PDO wskazał, że są one nadal potrzebne PDO w celu ustalenia, dochodzenia lub obrony roszczeń PDO,
- d) PDO wniesie sprzeciw wobec przetwarzania jego Danych Osobowych, a ADO nie stwierdzi nadrzędnych prawnie uzasadnionych podstaw do przetwarzania ich w pełnym zakresie.

4.12.6.2. Koordynator ds. ODO zobowiązuje właścicieli poszczególnych zbiorów do zidentyfikowania Danych Osobowych, których przetwarzanie powinno być ograniczone, w rozsądnym terminie, nie dłuższym niż 2 tygodnie. Koordynator ds. ODO przekazuje właścicielom poszczególnych Zbiorów, w których są przetwarzane Dane Osobowe podlegające ograniczeniu informację o obowiązku ograniczenia ich przetwarzania.

4.12.6.3. Dane Osobowe objęte uprawnieniem do ograniczenia przetwarzania można przetwarzać wyłącznie w zakresie przechowywania, bez możliwości wykonywania innych operacji przetwarzania, chyba że uzyskana zostanie wyraźna zgoda PDO lub jest to niezbędne dla ustalenia, dochodzenia lub obrony roszczeń, w celu ochrony praw innej niż PDO osoby, lub z uwagi na ważne względy interesu publicznego. Ograniczenie przetwarzania realizowane jest poprzez przeniesienie Danych do osobnej bazy niepodlegającej bieżącym operacjom przetwarzania lub poprzez maskowanie Danych tak, by były one niewidoczne w systemie i nie podlegały dalszemu przetwarzaniu.

4.12.6.4. Koordynator ds. ODO zobowiązany jest poinformować każdego Odbiorcę Danych podlegających ograniczeniu przetwarzana o wykonaniu tego prawa.

	4.12.6.5. Koordynator ds. ODO regularnie sprawdza, czy utrzymuje się podstawa do ograniczenia przetwarzania Danych Osobowych i w przypadku wygaśnięcia takiej podstawy zwraca się do właścicieli odpowiednich zbiorów o przywrócenie pełnego zakresu przetwarzania Danych Osobowych. 4.12.7. Obowiązki ADO w przypadku żądania w zakresie prawa do sprostowania lub uzupełnienia Danych. 4.12.7.1. Koordynator ds. ODO przekazuje właścicielom poszczególnych zbiorów, w których są przetwarzane Dane Osobowe podlegające sprostowaniu lub uzupełnieniu, a także wszystkim Odbiorcom Danych, informację o żądaniu ich sprostowania lub uzupełnienia, przekazując jednocześnie treść sprostowanych lub uzupełnianych Danych PDO. 4.12.7.2. Właściciele zbiorów i odbiorcy Danych weryfikują, czy przetwarzane Dane są aktualne i jeżeli wymagają sprostowania lub uzupełnienia zgodnie z żądaniem PDO – dokonują odpowiedniej zmiany, o czym informują Koordynatora ds. ODO, nie później niż w terminie jednego tygodnia. 4.12.7.3. Koordynator ds. ODO zobowiązany jest niezwłocznie poinformować każdego PDO o wykonaniu obowiązku sprostowania lub uzupełnienia jego Danych. 4.12.8. Obowiązki ADO w przypadku żądania w zakresie prawa do sprzeciwu wobec przetwarzania Danych Osobowych. 4.12.8.1. ADO zobowiązany jest uwzględnić: a) sprzeciw wobec przetwarzania: • niezbędnego do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej, • niezbędnego do celów wynikających z prawnie uzasadnionych interesów realizowanych przez ADO lub osobę trzecią, jeżeli nie istnieje nadrzędna prawnie uzasadniona podstawa przetwarzania, b) sprzeciw wobec przetwarzania Danych, które przetwarzane były na potrzeby marketingu bezpośredniego. 4.12.8.2. Do czasu rozstrzygnięcia sprzeciwu ADO zobowiązany jest ograniczyć przetwarzanie Danych objętych treścią sprzeciwu, wykonując czynności wskazane w punktach 4.12.6.2 – 4.12.6.5. 4.12.8.3. W przypadku uwzględnienia sprzeciwu ADO zobowiązany jest usunąć Dane objęte treścią sprzeciwu, wykonując czynności wskazane w punktach 4.12.5.2 – 4.12.5.6. 4.12.8.4. W zakresie, w jakim procesorzy zostali upoważnieni do przetwarzania Danych PDO, zostaną poinformowani niezwłocznie o wniesieniu sprzeciwu i poproszeni o potwierdzenie jego wypełnienia na piśmie lub w formie elektronicznej w terminie nie dłuższym niż jeden tydzień. 4.12.9. Obowiązki ADO w przypadku żądania w zakresie prawa do niepodlegania decyzji opierającej się wyłącznie na zautomatyzowanym przetwarzaniu. 4.12.9.1 ADO zobowiązany jest w każdym przypadku dążyć do tego, by decyzje dotyczące PDO nie były podejmowane wyłącznie w sposób zautomatyzowany. 4.12.9.2 W przypadku, gdy w toku procesów przetwarzania zidentyfikowana zostanie sytuacja, gdy decyzja wobec PDO podejmowana jest wyłącznie w sposób zautomatyzowany, ADO przed wystąpieniem skutków takiej decyzji poinformuje o jej podjęciu PDO, a także o możliwości wyrażenia stanowiska przez PDO, w tym zakwestionowania decyzji. ADO poda przy tym adres e-mail, za pośrednictwem którego PDO może wykonać te uprawnienia. 4.12.9.3 W przypadku zakwestionowania decyzji przez PDO, ADO wstrzyma wykonanie tej decyzji i zapewni, podjęcie jej jeszcze raz przez człowieka w sposób niezautomatyzowany. O treści podjętej w ten sposób decyzji PDO zostanie niezwłocznie poinformowany za pośrednictwem poczty e-mail na adres, za pomocą którego PDO wykonywał swoje uprawnienia.
Nr 4.13	**Szkolenia** 4.13.1. Administrator organizuje szkolenie dla osób upoważnionych do przetwarzania Danych Osobowych w zakresie obowiązujących przepisów, procedur oraz podstawowych zagrożeń związanych z przetwarzaniem Danych. 4.13.2. Szkolenie w miarę możliwości jest przeprowadzane przed dopuszczeniem osoby upoważnionej do czynności przetwarzania Danych oraz przed nadaniem upoważnienia. 4.13.3. Szkolenia prowadzi Administrator, Koordynator ds. ODO, IOD lub wybrana przez ADO osoba posiadająca wiadomości specjalne z zakresu ochrony Danych. 4.13.4. Przeprowadzenie szkolenia może być dokumentowane stosownymi zaświadczeniami.
Nr 4.14	**Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych** 4.14.1. Każdy, kto przetwarza Dane Osobowe obowiązany jest zachować w tajemnicy Dane Osobowe, do których posiada dostęp, sposoby zabezpieczania Danych jak również wszelkie informacje, które powziął w czasie przetwarzania Danych, zarówno w sposób zamierzony jak i przypadkowy. Obowiązek zachowania Danych w tajemnicy jest bezterminowy. 4.14.2. Podczas przetwarzania Danych należy zachować szczególną ostrożność i podjąć wszelkie możliwe środki umożliwiające zabezpieczenie oraz ochronę Danych przed nieuprawnionym dostępem, modyfikacją, zniszczeniem lub ujawnieniem. 4.14.3. Hasła i loginy, a także inne stosowane mechanizmy uwierzytelniające dostęp do systemu informatycznego nie mogą być ujawniane nawet po utracie ich ważności. 4.14.4. Należy dochować należytej staranności podczas przesyłania dokumentów zawierających Dane za pomocą środków komunikacji elektronicznej, w szczególności należy upewnić się czy przesyłane za pomocą poczty elektronicznej dokumenty trafiły do właściwego odbiorcy. 4.14.5. W przypadku przesyłania za pomocą środków komunikacji elektronicznej dokumentów, zestawień, spisów zawierających Dane Osobowe, przesyłany dokument należy zaszyfrować, a hasło przesłać, w miarę możliwości innym środkiem komunikacji elektronicznej.

	4.14.6. Osoba będąca dysponentem kluczy nie może przekazywać kluczy do budynków i pomieszczeń, w których przetwarzane są Dane osobom nieuprawnionym, a ponadto obowiązana jest przedsięwziąć działania celem wykluczenia ryzyka ich utraty. 4.14.7. Osoba, która utraciła posiadane klucze do pomieszczeń ADO, w których przetwarzane są Dane, niezwłocznie zgłasza tą okoliczność do Koordynatora ds. ODO. 4.14.8. Koordynator ds. ODO podejmuje wszelkie niezbędne środki techniczne i organizacyjne w celu zabezpieczenia pomieszczenia, do którego klucze utracono. 4.14.9. Ogólny opis środków technicznych i organizacyjnych stosowanych przez ADO celem zapewnienia poufności, integralności i rozliczalności Przetwarzanych Danych zawarty został w *Rejestrze czynności przetwarzania (Formularz III.E.1-F3).* 4.14.10. Użytkownik po zakończeniu pracy porządkuje swoje stanowisko zabezpieczając dokumenty i nośniki elektroniczne z Danymi w specjalnie do tego przeznaczonych szafach, zamykanych na klucz szafkach, szufladach lub pomieszczeniach. 4.14.11. Niszczenie dokumentów zawierających Dane odbywa się jedynie za pomocą niszczarki gwarantującej odpowiedni stopień rozdrobnienia (zaleca się, aby niszczarka spełniała wymogi normy DIN 66399, klasa bezpieczeństwa nie niższa niż 3) lub za pośrednictwem firmy zajmującej się niszczeniem dokumentów, po zawarciu Umowy Powierzenia przetwarzania Danych Osobowych. 4.14.12. Każdy dokument zawierający Dane, a nieużyteczny, niszczy się niezwłocznie. 4.14.13. Podczas korzystania z urządzeń wielofunkcyjnych należy zachować szczególną ostrożność. Dokumenty kopiowane bądź skanowane wyjmowane są z urządzenia wielofunkcyjnego niezwłocznie po ich użyciu. Dotyczy to również dokumentów powstałych na skutek kopiowania bądź skanowania. 4.14.14. Przebywanie osób trzecich w obszarze, w którym przetwarzane są Dane jest dopuszczalne za zgodą ADO lub w obecności osoby upoważnionej. 4.14.15. Szczegółowy opis środków bezpieczeństwa zastosowanych przez ADO wskazany został w *Rejestrze czynności przetwarzania (Formularz III.E.1-F3).* 4.14.16. Sposób zarządzania systemem informatycznym, służącym do przetwarzania Danych Osobowych oraz stosowanych zabezpieczeń został opisany w *Procedurze III.E.2 Instrukcja zarządzania systemem informatycznym*.
Nr 4.15	**Postępowanie w razie incydentów stanowiących naruszenie ODO** 4.15.1. Ogólne obowiązki w zakresie naruszeń. 4.15.1.1. W przypadku faktycznego lub potencjalnego naruszenia ODO lub uzasadnionego podejrzenia naruszenia ODO każda osoba upoważniona, a także każda inna osoba, która dowiedziała się, że mogło lub może dojść do takiego naruszenia, zobowiązana jest: a) powstrzymać się od rozpoczęcia lub od kontynuowania jakichkolwiek czynności mogących spowodować zatarcie śladów bądź dowodów związanych z danym naruszeniem ODO; b) podjąć niezbędne działania aby zapobiec eskalacji naruszenia ODO; c) podjąć niezbędne działania aby zabezpieczyć te elementy systemu informatycznego, zbioru Danych Osobowych lub samych Danych, które na tym etapie nie zostały objęte naruszeniem ODO; d) niezwłocznie, nie dłużej niż w ciągu 2 godzin, powiadomić Koordynatora ds. ODO o danym naruszeniu ODO: • poprzez zgłoszenie w systemie Axence nVision, lub • przesyłając pocztą elektroniczną formularz *Powiadomienie o naruszeniu ODO*, którego wzór zawarto w *Formularzu III.E.1-F7*, lub • telefonicznie/osobiście; e) dodatkowo powiadomić bezpośredniego przełożonego w strukturze organizacyjnej. 4.15.1.2. Niezwłocznie po otrzymaniu zawiadomienia o naruszeniu ODO lub stwierdzeniu wystąpienia takiego naruszenia ODO, Koordynator ds. ODO zobowiązany jest podjąć następujące działania: a) zidentyfikować źródło powstania naruszenia ODO i w tym czasie, o ile to możliwe wstrzymać prowadzenie działalności, która skutkuje dalszą eskalacją naruszenia ODO, b) opracować rozwiązanie usuwające źródło i skutki naruszenia ODO, c) zakomunikować wszystkim osobom, które zobowiązane są do podejmowania czynności związanych z wdrożeniem rozwiązania o czynnościach, jakie muszą wykonać w celu usunięcia źródła i skutków naruszenia ODO, udokumentować okoliczności i przebieg wystąpienia, skutki oraz działania podjęte w celu usunięcia Naruszenia ODO – za pomocą *Rejestru Naruszeń ODO* prowadzonego według wzoru stanowiącego *Formularz III.E.1-F8,* d) dokonać zawiadomień, których mowa w punktach 4.15.2 i 4.15.3. 4.15.1.3. Koordynator ds. ODO niezwłocznie powiadamia o naruszeniu ODO również Zarząd ADO. 4.15.1.4. Zgłoszenie naruszenia ODO do Organu Nadzorczego oraz do Zarządu ADO powinno zawierać: a) opis charakteru naruszenia ODO, w tym: kategorie i liczbę osób, których dotyczą Dane Osobowe objęte naruszeniem ODO, kategorie i liczbę wpisów Danych Osobowych, których dotyczy naruszenie ODO, b) imię, nazwisko oraz dane kontaktowe Koordynatora ds. ODO lub innego punktu kontaktowego, c) możliwe konsekwencje naruszenia ODO, d) środki zastosowane lub proponowane przez ADO celem zaradzenia naruszeniu ODO, w tym w celu zminimalizowania skutków naruszenia ODO. 4.15.2. Zawiadomienie PDO. 4.15.2.1. W przypadku naruszenia ODO, Koordynator ds. ODO każdorazowo dokonuje oceny, czy na skutek naruszenia dochodzi do wysokiego ryzyka naruszenia praw lub wolności PDO. Przy dokonywaniu oceny Koordynator ds. ODO bierze każdorazowo pod uwagę, czy zachodzi któraś z okoliczności wskazanych w punkcie 4.15.3.3 poniżej. W przypadku stwierdzenia takiego ryzyka, Koordynator ds. ODO bez zbędnej zwłoki zawiadamia Zarząd ADO. Zarząd ADO niezwłocznie podejmuje decyzję o zawiadomieniu PDO.

	4.15.2.2. Zawiadomienie kierowane do PDO powinno zawierać: a) opis charakteru naruszenia ODO prostym i jasnym językiem, b) imię, nazwisko oraz dane kontaktowe Koordynatora ds. ODO lub innego punktu kontaktowego, c) możliwe konsekwencje naruszenia ODO, d) środki zastosowane lub proponowane przez ADO celem zaradzenia naruszeniu ODO, w tym w celu zminimalizowania skutków naruszenia ODO. 4.15.2.3. Zawiadomienie nie jest wymagane, gdy wystąpiła co najmniej jedna z poniższych sytuacji: a) ADO wdrożył odpowiednie techniczne i organizacyjne środki ochrony uniemożliwiające odczyt danych osobom nieuprawnionym (np. szyfrowanie), i środki te zostały zastosowane do Danych Osobowych PDO, których dotyczy naruszenie ODO, b) ADO zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności PDO, c) zawiadomienie PDO wymagałoby niewspółmiernie dużego wysiłku – w takim przypadku, każdorazowo po uprzedniej konsultacji z Zarządem ADO, wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek poinformowania PDO. 4.15.2.4. Koordynator ds. ODO zawiadamia PDO o naruszeniu ODO obowiązkowo, jeżeli zażąda tego Organ Nadzorczy. Koordynator ds. ODO zawsze informuje o takim żądaniu Zarząd ADO. 4.15.3. Konsekwencje naruszenia obowiązków. 4.15.4. Wobec podmiotów nieprzestrzegających niniejszych postanowień, ADO może wyciągnąć konsekwencje dyscyplinarne lub przewidziane przepisami prawa, łącznie z rozwiązaniem stosownych umów, roszczeniami odszkodowawczymi lub zgłoszeniem incydentu odpowiednim władzom państwowym.
Nr 4.16	**Postępowanie w razie incydentów związanych z naruszeniem postanowień procedur ODO nieskutkujących naruszeniem ODO** 4.16.1. W przypadku naruszenia lub uzasadnionego podejrzenia naruszenia postanowień Procedur ODO nieskutkującego faktycznym lub potencjalnym naruszeniem ODO każda osoba zobowiązana jest niezwłocznie powiadomić o danym incydencie telefonicznie oraz pocztą elektroniczną Koordynatora ds. ODO oraz, o ile występuje, bezpośredniego przełożonego w strukturze organizacyjnej ADO. Osoby trzecie winny natychmiast zawiadomić ADO. 4.16.2. Wobec podmiotów nieprzestrzegających postanowień Procedur ODO, ADO może wyciągnąć konsekwencje dyscyplinarne lub przewidziane przepisami prawa, łącznie z rozwiązaniem stosownych umów, roszczeniami odszkodowawczymi lub zgłoszeniem incydentu odpowiednim władzom państwowym.
Nr 4.17	**Dodatkowe informacje** 4.17.1. Dokumentacja przetwarzania Danych Osobowych stanowi wewnętrzną regulację ADO i obowiązuje cały personel ADO. 4.17.2. Dokumentacja przetwarzania Danych Osobowych obowiązuje od dnia jej wprowadzenia w życie w sposób przyjęty u ADO. Wszelkie zmiany dokumentacji przetwarzania Danych Osobowych obowiązują od dnia ich wprowadzenia w życie w sposób przyjęty u ADO. 4.17.3. Każdy kto przetwarza Dane posiadane przez ADO zobowiązany jest do stosowania przy przetwarzaniu Danych Osobowych postanowień zawartych w niniejszej dokumentacji przetwarzania Danych Osobowych oraz w *Procedurze III.E.4. Regulamin Użytkownika systemów informatycznych*. 4.17.4. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub niewykonanie zobowiązania w przypadku stosunku prawnego innego niż stosunek pracy. W sprawach nieuregulowanych w niniejszej polityce bezpieczeństwa mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym w szczególności przepisy RODO.
5. DOKUMENTY WZORCOWE / FORMULARZE I ICH UŻYKOWNICY	III.E.1-F1 – Umowa powierzenia /wzór/ – *Koordynator ds. ODO, Dyrektorzy/Menadżerowie/Liderzy/Kierownicy Projektu* III.E.1-F2 – Rejestr umów powierzenia /wzór/ – *Koordynator ds. ODO* III.E.1-F3 – Rejestr czynności przetwarzania /wzór/ – *Koordynator ds. ODO* III.E.1-F4a – Upoważnienie i oświadczenie – na czas obowiązywania umowy o pracę /wzór/ - *Koordynator ds. ODO, Dyrektorzy/Menadżerowie/Liderzy/Kierownicy Projektu* III.E.1-F4b – Upoważnienie i oświadczenie – na czas obowiązywania umowy zlecenia, o dzieło, współpracy B2B /wzór/ – *Koordynator ds. ODO, Dyrektorzy/Menadżerowie/Liderzy/Kierownicy Projektu* III.E.1-F4c – Upoważnienie i oświadczenie – na czas realizacji projektu /wzór/ – *Koordynator ds. ODO, Dyrektorzy/Menadżerowie/Liderzy/Kierownicy Projektu* III.E.1-F5 – Ewidencja zbiorów i osób upoważnionych /wzór/ – *Koordynator ds. ODO* III.E.1-F6 – Protokół przyjęcia i realizacji żądania PDO /wzór/ – *Osoba upoważniona do przetwarzania danych* III.E.1-F7 – Powiadomienie o naruszeniu ODO /wzór/ – *Osoba upoważniona do przetwarzania danych* III.E.1-F8 – Rejestr naruszeń ODO /wzór/ – *Koordynator ds. ODO* III.E.1-F9 – Protokół z kontroli wewnętrznej ODO /wzór/ – *Koordynator ds. ODO oraz ASI* III.E.1-F10 – Raport z oceny nowego systemu informatycznego /wzór/ – *Koordynator ds. ODO oraz ASI* III.E.1-F11 – Sprawozdanie z oceny skutków /wzór/ – *Koordynator ds. ODO oraz ASI* III.E.1-F12 – Rejestr kategorii czynności przetwarzania /wzór/ – *Koordynator ds. ODO* III.E.1-F13 – Standardowe klauzule umów powierzenia danych osobowych poza UE – *Koordynator ds. ODO* III.E.1-F14 – Klauzule informacyjne dla PDO – Koordynator ds. ODO III.E.1-F15 – Umowa podpowierzenia /wzór/ – *Koordynator ds. ODO, Dyrektorzy/Menadżerowie/Liderzy/Kierownicy Projektu*
6. ZAŁĄCZNIKI	III.E.1-Z1 – Zasady postępowania z informacjami w wersji papierowej III.E.1-Z2 – Polityka prywatności serwisu internetowego

Załącznik III.E.1-Z1 Zasady postępowania z informacjami w wersji papierowej

MGGP GRUPA MGGP	Zasady postępowania z informacjami w wersji papierowej		
Wersja: 02	Kategoria jawności: II (wewnętrzne)	Obowiązuje od: 01.02.2024 r.	Stron: 3

1. Cele określania standardu postępowania z informacjami/nośnikami w wersji papierowej.

1.1 Instrukcja ma zapewnić redukcję ryzyka utraty poufności lub integralności danych w trakcie pracy w biurze, transporcie, w czasie przekazywania pomiędzy członkami zespołu oraz w związku z przesyłaniem danych firmom zewnętrznym.
1.2 Instrukcja ma ułatwić późniejsze usuwanie lub ograniczanie przetwarzania danych osobowych, w związku z realizacją pierwotnego celu przetwarzania, zaniknięciem podstawy prawnej przetwarzania lub na wniosek osoby, której dane dotyczą.
1.3 Instrukcja ma umożliwić niezależne zarządzanie uprawnieniami dostępowymi, do wglądu lub edycji, do danych w związku ze zmianą celu ich przetwarzania (chodzi o przeniesienie danych z zasobów bieżąco procesowanych do zasobów przechowywanych dla celów archiwalnych lub w związku z ustaleniem, dochodzeniem lub obroną roszczeń).
1.4 Instrukcja ma gwarantować skuteczne usuwanie danych.
1.5 Instrukcja ma zwiększać zdolność dowodową w zakresie wykazania realizacji obowiązku ochrony danych osobowych.

2. Postępowanie z dokumentacją papierową w obiegu w ramach MGGP S.A.

2.1 Wszelkie dokumenty zawierające dane osobowe lub dane stanowiące wartość dla Organizacji, o ile istnieje konieczność ich przekazania innemu członkowi zespołu, powinno się przekazywać do rąk własnych tego członka.
2.2 W przypadku braku takiej możliwości, dokumenty należy przekazać na ręce bezpośredniego przełożonego tego członka, którego obowiązują te same zasady.
2.3 W przypadku opuszczania stanowiska pracy lub w związku z zakończeniem dnia pracy wszelkie dokumenty zawierające dane osobowe lub dane stanowiące wartość dla Organizacji, powinny zostać umieszczone w zamkniętym meblu.
2.4 Wszelkie dokumenty, wraz z upłynięciem okresu ich przydatności, należy niszczyć z wykorzystaniem niszczarki do dokumentów.
2.5 Wszelkie dokumenty, zawierające dane osobowe lub dane stanowiące wartość dla organizacji, należy przechowywać w teczkach, segregatorach, kartonach, wydzielonych szufladach lub innych pojemnikach oznaczonych w sposób pozwalający na identyfikację.
2.6 Z chwilą upłynięcia okresu przydatności dokumentów zawierających dane osobowe lub dane stanowiące wartość dla organizacji, należy o tym fakcie zawiadomić bezpośredniego przełożonego i na jego polecenie odpowiednio: przenieść dokumenty w miejsce do tego wyznaczone lub zdać osobie wyznaczonej do gromadzenia dokumentacji w celu ustalenia, dochodzenia lub obrony roszczeń (oznacza to wskazanie nowego celu przetwarzania dla danych zawartych w tej dokumentacji), zniszczyć dokumenty w niszczarce lub dokonać ich anonimizacji przez trwałe uniemożliwienie odczytania danych identyfikujących (w przypadku danych procesowanych na zlecenie, standard dalszego postępowania z nimi określa umowa przedmiotowa).
2.7 Zabrania się pozostawiania dokumentów zawierających dane osobowe lub dane stanowiące wartość dla Organizacji na biurku w momencie opuszczania biura oraz przekazywania dokumentów innym osobom poprzez położenie ich na biurku tej innej osoby pod jej nieobecność; spod stosowania powyższej zasady **wyłączone są** wizytówki oraz inne dokumenty zawierające nieuporządkowane dane o analogicznej zawartości (np. kartki typu sticker z danymi osoby oczekującej na informację, kalendarz itd.).
2.8 Zabrania się wyrzucania do śmieci **wszelkich** dokumentów zawierających dane osobowe lub dane stanowiące wartość dla Organizacji.
2.9 Każdy pracownik powinien zawsze znać przeznaczenie każdego dokumentu znajdującego się w jego posiadaniu.

3. Postępowanie z dokumentacją papierową przetwarzaną poza biurem Administratora.

3.1 Wszelkie dokumenty zawierające dane osobowe i przeznaczone do wyniesienia poza biuro Organizacji, należy na początku przygotować do transportu poprzez ich przeniesienie do nieprzezroczystych teczek, kopert lub segregatorów.
3.2 Zabrania się Personelowi korzystania z dokumentów papierowych w obecności osób trzecich (czyli osób, których dane te nie dotyczą oraz które nie są zaangażowane w pracę na nich), a zwłaszcza innych klientów / kontrahentów oraz w miejscach publicznych, w sposób pozwalający na wgląd w te dane przez osoby nieuprawnione.
3.3 Zabrania się pozostawiania dokumentów zawierających dane osobowe w salach konferencyjnych po zakończeniu spotkania, chyba że sala ta zostanie zamknięta, a osoba sprawująca pieczę nad dokumentami ma gwarancję, że nie dojdzie do otwarcia pomieszczenia do jej powrotu (chodzi o sytuacje przerw w spotkaniach, negocjacjach, szkoleniach oraz o moment odprowadzania gości po zakończeniu spotkania itp.).

4. Prowadzenie ewidencji udostępnień.

4.1 Z uwagi na obowiązek gromadzenia materiału dowodowego dla celów rozliczalności, dokumenty w formie papierowej zawierające dane osobowe lub dane stanowiące wartość dla Organizacji, a przeznaczone do przekazania osobie nie będącej członkiem Personelu, podlegają ewidencjonowaniu na zasadach opisanych poniżej. Pod pojęciem przekazania rozumie się umożliwienie Odbiorcy wyniesienia danych (dokumentu źródłowego albo jego kopii) poza siedzibę Administratora. Obowiązek ewidencjonowania występuje również w przypadku przekazania dokumentów organowi publicznemu, jeżeli otrzymuje on dokumenty w ramach konkretnego postępowania, na podstawie odpowiednich przepisów prawa. **Przekazaniem nie jest** umożliwienie wglądu w pomieszczeniach Organizacji, np. w sytuacji audytu lub kontroli.
4.2 Ewidencja dokumentów przekazywanych poza Organizację w taki sposób, że Administrator traci nad nimi kontrolę prowadzona jest w postaci arkusza Excel przez asystenta/wyznaczonego pracownika w każdej jednostce organizacyjnej Administratora.
4.3 W przypadku możliwości przekazania kopii dokumentu papierowego i dostateczności takiej formy dla celów przetwarzania, należy przekazać kopię dokumentu, a fakt ten odnotować.
4.4 W przypadku, w którym niezbędne jest przekazanie oryginału dokumentu, należy przed przekazaniem wykonać jego kopię, a fakt przekazania oryginału należy odnotować oraz ustalić datę jego zwrotu.
4.5 Ewidencja zawiera co najmniej następujące informacje:
a) informacje jednoznacznie identyfikujące dokument (nadawca/autor, data, sygnatura/znak/numer dokumentu, zwięzłe wskazanie przedmiotu/nazwa dokumentu),
b) wskazanie danych podlegających przekazaniu,
c) wskazanie podmiotu, któremu dane zostały przekazane,
d) datę przekazania,
e) podstawę faktyczną i, jeżeli dotyczy, prawną przekazania,
f) datę planowanego i faktycznego zwrotu,
g) dla dokumentów zapakowanych w sposób uniemożliwiających kontrolę treści wpisuje się wyłącznie dane nadawcy oraz przedmiot sprawy, o ile jest znany.

4.6 Personel przekazujący dokumenty zawierające dane osobowe lub dane stanowiące wartość dla Organizacji, informują o przekazaniu dokumentów asystenta/wyznaczonego pracownika w danej jednostce organizacyjnej Administratora, który wprowadza taką informację do ewidencji.
4.7 Spod obowiązku ewidencjonowania wyjęte są wszelkie dokumenty, których zawartość jasno wynika z ich formy lub sprawy, której dotyczą, takie jak:
a) zestandaryzowane zgłoszenia, powiadomienia lub wnioski (np. listy przewozowe itd.),
b) opracowane na podstawie obowiązujących druków / wzorów (np. zgłoszenie pracownika do ZUS, US itd.),
c) wszelkie inne, jeżeli zakres danych osobowych w nich zawarty nie przekracza standardowego zakresu informacji przekazywanych zwykle kontrahentom / podmiotom trzecim (np. numer telefonu, e-mail, siedziba biura) widniejących na wizytówce.

5. Zasady wysyłania dokumentów zawierających dane osobowe lub dane chronione przez Organizację za pośrednictwem: Poczty Polskiej, Firm kurierskich, członków Personelu.
5.1. W przypadku przesyłania dokumentacji należy korzystać z zaufanych operatorów, a przesyłki należy wysyłać za pokwitowaniem.
5.2. Osoby przekazujące dokumenty do wysyłki przedstawicielowi poczty lub kurierowi powinna posiadać pewność, że dana osoba reprezentuje konkretnego operatora.
5.3. Wysyłane dokumenty należy zarejestrować w ewidencji korespondencji wychodzącej.
5.4. Dokumenty przeznaczone do wysyłki pocztą lub przesyłką kurierską lub za pośrednictwem członków Personelu oczekują na wysyłkę w postaci zapakowanej.
5.5. Dokumenty powinny zostać odpowiednio zabezpieczone przed zniszczeniem oraz dostępem osób trzecich.
5.6. Dokument, który przeznaczony jest do konkretnego adresata powinien zostać oznaczony na kopercie pieczątką lub odręcznym napisem „dostarczyć do rąk własnych" ze wskazaniem tego adresata.
5.7. Niezależnie od formy wysyłki dokumentu, jego nadawca winien upewnić się, że dokument dotarł do adresata.

UWAGA:
Przekazywanie przedstawicielowi poczty lub firmy kurierskiej danych osobowych odbiorców przesyłek przez niego doręczanych w formie etykiet adresowych i/lub listy nie wymaga odrębnej zgody osoby, której dane dotyczą, ponieważ doręczenie przesyłki za pośrednictwem kuriera jest elementem przetwarzania danych, które ma inną podstawę prawną. Nie zwalnia to operatorów pocztowych ani firm kurierskich z obowiązku należytej ochrony przekazanych im w ten sposób danych osobowych.

6. Postępowanie z dokumentacją papierową przetwarzaną poza biurem Administratora podczas pracy na odległość.
6.1. Administrator wdrożył elektroniczny obieg dokumentów, a Personel ma bezpieczny dostęp do niezbędnych do pracy danych osobowych i danych mających wartość dla Organizacji, przy pomocy środków komunikacji elektronicznej podczas wykonywania pracy na odległość rozumianej jako praca poza siedzibą/lokalizacjami/lub wyznaczonymi biurami tymczasowymi Organizacji, m.in. przy wykonywaniu pracy zdalnej w rozumieniu przepisów prawa pracy. Administrator może także udostępnić Personelowi odpowiednio zabezpieczone (m.in. zaszyfrowane) elektroniczne kopie niezbędnych dokumentów.
6.2. W sytuacji, gdy praca na odległość na dokumentach w wersji elektronicznej nie jest możliwa, a do wykonania pracy Personelowi niezbędny jest dostęp do danych osobowych lub danych mających wartość dla Organizacji w wersji papierowej, w wyjątkowych sytuacjach Administrator może wyrazić zgodę na wynoszenie przez Personel poza biuro Administratora dokumentacji papierowej, tylko na czas wykonywania pracy na odległość i wyłącznie w odniesieniu do dokumentów niezbędnych. Zgodę taką w imieniu Administratora, w formie pisemnej lub drogą elektroniczną, wyraża przełożony pracownika. Jednakże zgoda taka może również wynikać:
a) bezpośrednio z umowy, w której wpisano adres wykonywania pracy inny niż siedziba organizacji, lub
b) z rodzaju umowy (np. umowa o telepracę), lub
c) z zarządzenia/uchwały ADO.
6.3. Personel w sytuacji określonej w ust. 2 podczas pracy na odległość pracuje na kopiach dokumentów, z zastrzeżeniem sytuacji, gdy praca na kopiach dokumentów nie jest możliwa.
6.4. Udostępnione dokumenty są przechowywane przez Personel przez okres niezbędny do wykonania określonego zadania podczas pracy na odległość.
6.5. Administrator ogranicza liczbę dokumentów wynoszonych z siedziby Administratora do tego, co niezbędne w stosunku do celu przetwarzania danych osobowych przez Personel w ramach pracy na odległość.
6.6. Za bezpieczeństwo dokumentów i wydruków zawierających dane chronione (w tym dane osobowe i dane stanowiące wartość dla Organizacji) odpowiedzialne są osoby, które korzystają z dokumentów papierowych w czasie pracy na odległość oraz Dyrektorzy/Menadżerowie właściwych jednostek organizacyjnych.
6.7. Podczas pracy na odległość członkowie Personelu nie mogą samowolnie wynosić dokumentacji w postaci papierowej poza określony przez pracodawcę obszar pracy na odległość.
6.8. Wydawane dokumenty papierowe na czas pracy na odległość podlegają ewidencjonowaniu. Ewidencja ta prowadzona jest w postaci arkusza Excel. Ewidencja zawiera informacje o tym, kto otrzymał dokumenty, jakie to były dokumenty, kiedy miało miejsce przekazanie, czy wydana została kopia czy oryginał dokumentu, okres na jaki wydaje się dokumenty. Ewidencję prowadzi Asystent/wyznaczony pracownik w każdej jednostce organizacyjnej.
6.9. Personel przetwarzając dane osobowe lub dane mające wartość dla Organizacji podczas pracy na odległość zobowiązuje się zapewnić ich bezpieczeństwo, stosując niżej opisane zasady, niezależnie czy pracuje na kopiach, czy na oryginałach dokumentów:
a) Personel zobowiązany jest do przewożenia dokumentów w sposób zapobiegający ich ujawnieniu, kradzieży, zagubieniu, utracie lub uszkodzeniu,
b) zabrania się Personelowi korzystania z dokumentów papierowych w obecności osób trzecich (czyli osób, których dane te nie dotyczą oraz które nie są zaangażowane w pracę na nich), a zwłaszcza innych klientów / kontrahentów, członków rodziny oraz w miejscach publicznych w sposób pozwalający na wgląd w te dane przez osoby nieuprawnione,
c) dokumenty i wydruki zawierające dane chronione przechowuje się w pomieszczeniach zabezpieczonych fizycznie przed dostępem osób nieupoważnionych,
d) Personel zobowiązany jest do stosowania polityki czystego biurka – polega ona na zabezpieczaniu dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych,
e) Personel zobowiązany jest do przestrzegania Polityki Ochrony Danych osobowych obowiązującej w MGGP S.A. wraz z dokumentami powiązanymi,
f) Personel wykorzystuje pozyskane dane osobowe i inne dane stanowiące wartość dla Organizacji wyłącznie w tym celu, w jakim byłyby wykorzystywane w siedzibie zakładu pracy,
g) Personel zobowiązany jest do niszczenia niepotrzebnych dokumentów i wydruków w sposób bezpieczny w dedykowanych temu niszczarkach; w sytuacji gdy dana osoba nie posiada w domu niszczarki, powinien dokumenty przechować w bezpieczny sposób, a po zakończeniu pracy na odległość zniszczyć je w biurze,

h) Personel zobowiązany jest zgłaszać każdy incydent bezpieczeństwa zgodnie z procedura postępowania w sprawie naruszeń ochrony danych, tak aby Administrator mógł się wywiązać z obowiązku nałożonego na mocy art. 33 ust. 1 RODO.

7. Zmiana celu przetwarzania – przeniesienie dokumentów z zasobów procesowanych do zasobów przechowywanych dla celów archiwalnych lub w celu ustalenia, dochodzenia lub obrony roszczeń.

Z chwilą zakończenia zadania, projektu lub współpracy z danym kontrahentem, osoba prowadząca ten proces zawiadamia o tym fakcie bezpośredniego przełożonego, który podejmuje decyzję odpowiednio o anonimizacji, archiwizacji lub usunięciu danych. W sytuacji kiedy umowa, na podstawie której realizowany był proces, definiuje sposób postępowania z danymi po jego zakończeniu należy przestrzegać również jej postanowień.

Procedura III.E.2 Instrukcja zarządzania systemem informatycznym

Właściciel procesu: Administrator Systemów Informatycznych			
Wersja: 02	Kategoria jawności: II (wewnętrzne)	Obowiązuje od: 08.02.2022 r.	Stron: 6

1. CEL I PRZEDMIOT PROCEDURY	Celem dokumentu jest opisanie zasad zarządzania aktywami informatycznymi przetwarzającymi Dane Osobowe oraz innymi systemami informatycznymi mającymi wartość dla Organizacji. Dokument obowiązuje w szczególności osoby odpowiedzialne za nadzorowanie sprzętu komputerowego i infrastruktury IT (ASI i inne wyznaczone osoby). Instrukcja stanowi wykaz procedur oraz stosowanych środków technicznych i organizacyjnych mających na celu, zgodnie z art. 32 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/W (dalej RODO), zabezpieczyć przetwarzane Dane Osobowe. Administrator Danych Osobowych jest zobowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych Danych Osobowych, odpowiednią do zagrożeń oraz kategorii Danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. ADO zobowiązany jest zapewnić kontrolę nad tym, jakie Dane Osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. W tym celu prowadzona jest dokumentacja opisująca sposób przetwarzania Danych oraz środki zapewniające należytą ochronę.
2. UCZESTNICY I ROLE W PROCEDURZE	**a) ASI (lub upoważnieni przez niego pracownicy Dział IT):** - nadaje dostęp Użytkownikowi do systemów informatycznych, - prowadzi ewidencję urządzeń i aktywów informacyjnych, - zapewnia odpowiednią konfigurację stanowiska komputerowego lub innych aktywów zgodnie z wymaganiami ochrony Danych Osowych i wymaganiami systemu bezpieczeństwa informacji, - nadaje dostęp do systemów operacyjnych, aplikacji, baz danych, współpracuje w tym zakresie z Koordynatorem ds. ODO, - dokonuje przeglądu kont i uprawnień w administrowanych systemach, - zobowiązany jest do stosowania zabezpieczeń kryptograficznych, gromadzi informacje potrzebne do odzyskiwania zainstalowanych stanowisk komputerowych, - udziela niezbędnego wsparcia w zakresie stosowania technik kryptograficznych, - nadzoruje i kontroluje dostęp do miejsca przechowywania sprzętu serwerowego, urządzeń sieciowych, przechowywania danych i in., dokonuje konserwacji sprzętu, - nadzoruje wykorzystanie zasobów systemów, - nadzoruje wprowadzanie zmian w aktywach, - sprawuje nadzór nad licencjami, - odpowiada za instalację oprogramowania antywirusowego, - monitoruje źródła informacji o zagrożeniach dla bezpieczeństwa Danych Osobowych, - prowadzi okresowe przeglądy systemów informatycznych, - nadzoruje kopie zapasowe oraz poprawność ich wykonania, - jest odpowiedzialny za zapewnienie bezpieczeństwa sieci, - odpowiada za dokumentowanie i analizę zgłoszeń pod względem skutków bezpieczeństwa informacji, w przypadku wystąpienia incydentu w zakresie bezpieczeństwa Danych Osobowych niezwłocznie powiadamia Koordynatora ds. ODO; **b) Użytkownik systemów informatycznych:** - informuje Dział IT o zagrożeniach wskazywanych przez oprogramowanie antywirusowe, - odpowiada za posiadane nośniki, - zgłasza ASI zdarzenia dotyczące bezpieczeństwa informacji; **c) Menadżerowie/Dyrektorzy/Liderzy:** - wnioskują do ASI o przydzielenie dostępu Użytkownikowi systemu informatycznego lub zmianę w przydzielonych Użytkownikowi uprawnieniach, **d) Obszar Wsparcia:** - prowadzi ewidencję licencji jako wartości niematerialnych i prawnych w ewidencji środków trwałych i przechowuje dowody udzielonych licencji, - zapewnia ograniczenie dostępu fizycznego do pomieszczeń ze sprzętem, - zapewnia nadzór nad pracą osób trzecich w pomieszczeniach ze sprzętem, - zapewnia konserwację i okresowe przeglądy systemów wspomagających w pomieszczeniach ze sprzętem (ochrona ppoż., klimatyzacja, podtrzymanie napięcia i zasilanie awaryjne). **e) Zespół programistów:** - realizuje projekty zgodnie z Polityką bezpieczeństwa w rozwoju systemów i aplikacji.
3. TERMINOLOGIA	Definicje stosowane w niniejszym dokumencie zawarte są w słowniku.
1. INSTRUKCJE POSTĘPOWANIA	
Nr 4.1	**Zabezpieczenie systemów informatycznych** 1.1.1. Przyznanie dostępu Użytkownikowi do systemów informatycznych przetwarzających Dane Osobowe oraz innych systemów mających wartość dla Organizacji odbywa się dwuetapowo: etap pierwszy jest to etap uwierzytelnienia oraz autoryzacji Użytkownika systemu informatycznego za pomocą domeny MS Windows. Drugi etap polega na identyfikacji Użytkownika w konkretnym systemie przetwarzania Danych Osobowych lub innych systemie mającym wartość dla Organizacji. 1.1.2. Każdy system informatyczny pracujący w sieci posiada zainstalowany oraz aktualizowany automatycznie system antywirusowy. 1.1.3. Użytkownicy systemu informatycznego niezwłocznie informują Dział IT o zagrożeniach wskazywanych przez oprogramowanie antywirusowe.

	1.1.4.	Każdy zbiór wczytywany do komputera, w tym także wiadomości email, musi być przetestowany programem antywirusowym. Niedopuszczalne jest stosowanie dostępu do sieci Internet bez aktywnej ochrony antywirusowej oraz zabezpieczenia przed dostępem szkodliwego oprogramowania.
	1.1.5.	Użytkownicy urządzeń przenośnych, na których są przetwarzane Dane Osobowe lub inne dane mające wartość dla Organizacji, wynoszonych poza obszar Organizacji, są zobowiązani do przestrzegania zasad bezpieczeństwa opisanych w Procedurze III.E.4. Regulamin Użytkownika systemów informatycznych.
	1.1.6.	W przypadku użycia komputerów przenośnych lub sprzętu mobilnego do zdalnego dostępu do zasobów wewnętrznej sieci przez Internet, stosuje się szyfrowanie tego połączenia z użyciem połączenia VPN.
	1.1.7.	W przypadku użycia komputerów przenośnych lub sprzętu mobilnego do zdalnego dostępu do zasobów wewnętrznej sieci przez Internet dokonuje się uwierzytelnienia: z użyciem loginu i hasła oraz poprzez autoryzację adresu IP.
	1.1.8.	W oddziałach organizacji zapewniono redundantne łącza internetowe.
	1.1.9.	Zapewniono rozliczalność operacji dla pracy w kluczowych aplikacjach i bazach danych.
	1.1.10.	W ramach rozliczalności logowane są operacje tworzenia, modyfikacji, usuwania, wglądu, eksportu do plików.
	1.1.11.	Kluczowe aplikacje i bazy zawierające Dane Osobowe zabezpieczono przed eksportem Danych do plików.
	1.1.12.	Zabezpieczono interfejsy programistyczne poprzez zmianę domyślnych loginów i haseł / wyłączenie dostępu zdalnego, gdy nie jest wymagany.
	1.1.13.	Zabezpieczono testowe wersje aplikacji poprzez zmianę domyślnych loginów i haseł / wyłączenie dostępu zdalnego, gdy nie jest wymagany.
	1.1.14.	Zastosowano szyfrowanie / tokenizację baz danych.
	1.1.15.	W kluczowych aplikacjach stosuje się terminację sesji.
	1.1.16.	Stosuje się szyfrowanie połączenia z serwerem pocztowym (SSL/TLS).
	1.1.17.	Na stronach www stosowane jest szyfrowanie połączeń internetowych z użyciem protokołu TLS/SSL.
	1.1.18.	Formularze kontaktowe na stronach www zabezpieczono protokołem TLS/SSL.
	1.1.19.	Formularze logowania na stronach www zabezpieczono protokołem TLS/SSL.
	1.1.20.	Dokonuje się aktualizacji oprogramowania (firmware / sterowniki) urządzeń sieciowych oraz innych (np. w urządzeniach jak: routery, switche, access pointy, firewalle, macierze, dyski NAS, drukarki, skanery).
	1.1.21.	Dokonywana jest konfiguracja urządzeń sieciowych (routery, switche, access pointy, firewalle, macierze, dyski NAS, drukarki, skanery i inne) w celu zabezpieczenia przed nieuprawnionym dostępem do nich (w tym zmiana domyślnych haseł na urządzeniach, zmiana domyślnych nazw kont administracyjnych w urządzeniach, konfiguracja portów na routerze).
	1.1.22.	Dokonuje się aktualizacji oprogramowania systemów i aplikacji (systemy operacyjne na stacjach roboczych / systemy operacyjne serwerów / przeglądarki www / CMS (Wordpress, Drupal, Joomla, Prestashop,) / Dedykowany CMS / Adobe / Flash / Java / inne). Aktualizacja dokonywana jest zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji (np. aktualizacje, service packi, łatki).
	1.1.23.	Monitorowane są usługi sieciowe na serwerach i stacjach roboczych (np. DHCP, DNS, SSH, http, telnet, FTP, SMTP, SNMP) oraz utrzymuje się niezbędne usługi oraz dezaktywuje pozostałe.
	1.1.24.	Zastosowano system antywirusowy na serwerze i końcówkach klienckich.
	1.1.25.	Zastosowano filtr antyspamowy.
	1.1.26.	Stosowany jest Firewall.
	1.1.27.	Zastosowano mechanizmy kontroli dostępu do sieci w postaci translacji adresów NAT.
	1.1.28.	Sieć bezprzewodową zabezpieczono protokołem WPA2 z szyfrowaniem 802.1x EAP.
	1.1.29.	W celu zapewnienia bezpieczeństwa istnieje separacja sieci wewnętrznej bezprzewodowej od sieci przeznaczonej dla gości.
	1.1.30.	Stosuje się zabezpieczenie baz i katalogów dostępnych z poziomu sieci przed indeksacją wyszukiwarek.
	1.1.31.	Pozostałe środki zabezpieczeń zostały określone w rejestrze obszarów przetwarzania Danych Osobowych.
Nr 4.2	**Zarządzanie aktywami informacyjnymi**	
	4.2.1.	Wszystkie aktywa informacyjne wspierające przetwarzanie Danych Osobowych oraz innych danych mających wartość dla Organizacji powinny być ewidencjonowane. W wykazie aktywów należy uwzględnić: • **Stanowiska komputerowe** (stacjonarne i przenośne), ich konfiguracje sprzętowe oraz zainstalowane oprogramowanie (na podstawie licencji posiadanych przez organizację), • **Sprzęt serwerowy** tj. komputery przeznaczone do utrzymywania aplikacji i systemów, wykorzystywanych przez wielu użytkowników, umieszczonych w specjalnych pomieszczeniach (serwerowniach); jego konfigurację sprzętową oraz wykaz zainstalowanego oprogramowania (na podstawie licencji posiadanych przez organizację), • **Urządzenia sieciowe** (np.: routery, firewall, switche, access pointy) i ich konfigurację sprzętową, • **Urządzenia przeznaczone do przechowywania Danych** (macierze, serwery plików itp.) i ich konfigurację sprzętową, • **Urządzenia peryferyjne** (np. drukarki, urządzenia wielofunkcyjne) przypisane do pomieszczenia lub umieszczone w pomieszczeniach wspólnych, • **Pozostały sprzęt elektroniczny** przypisany do użytkowników systemów informacyjnych (np. smartfony, tablety, nośniki, danych, zapisy z kamer itd.), • **Oprogramowanie licencjonowane** posiadane przez organizację na podstawie umów, faktur i innych dokumentów wystawionych na organizację wraz ze wskazaniem dokumentu określającego prawa licencyjne, • **Oprogramowanie** dopuszczonego do instalacji na stanowiskach komputerowych lub urządzeniach serwerowych na podstawie ogólnej licencji (np. GPL, freeware), • **Maszyny wirtualne** skonfigurowane w ramach urządzenia (lub grupy urządzeń) serwerowych, • **Systemy informatyczne** zapewniające usługę informatyczną (np. poczta elektroniczna) lub dostarczające aplikację Użytkownikom. • **Przestrzenie wirtualizacyjne** umożliwiające tworzenie i utrzymywania maszyn wirtualnych umieszczonych w określonych sieciach z określonymi dostępami. • **Istotne osoby** mające wiedze niezbędną dla zapewniania działania i dostępu do istotnych informacji.

	4.2.2 Prowadzona ewidencja powinna zapewnić przypisanie aktywu informacyjnego do osoby odpowiedzialnej (np.: Użytkownik, Przełożony Jednostki Organizacyjnej). 4.2.3 Ewidencja powinna być prowadzona w pliku *Aktywa i Rejestr ryzyka BI i ODO (Formularz III.E.3-F2)* – w zakładce Ewidencja aktywów. Dopuszcza się utrzymywanie kilku wykazów aktywów i odwoływanie się do nich w Ewidencji. 4.2.4 Prowadzona ewidencja urządzeń (np. stanowiska komputerowe) powinna zapewnić możliwość jednoznacznej identyfikacji urządzenia (np. poprzez numer umieszczony na obudowie). 4.2.5 Stanowiska komputerowe i inny sprzęt/aktywa wydawane są członkom personelu po potwierdzeniu przejęcia sprzętu/aktywa. Potwierdzenie wyszczególnia parametry przekazywanego sprzętu/aktywa. 4.2.6 ASI zapewnia odpowiednią konfigurację stanowiska komputerowego lub innych aktywów zgodnie z wymaganiami ochrony Danych Osobowych i wymaganiami systemu bezpieczeństwa informacji. Minimalne wymagania dla sprzętu to: a) dostęp do urządzenia jest zabezpieczony (np. hasło, kod PIN, blokada na podstawie linii papilarnych), b) nośnik Danych na urządzeniu jest zaszyfrowany, c) urządzenie ma włączone automatyczne aktualizacje systemu operacyjnego, d) urządzenie ma zainstalowany program antywirusowy i włączone automatyczne aktualizacje bazy sygnatur wirusów, e) konto systemowe Użytkownika jest kontem o ograniczonych uprawnieniach. 4.2.7. Powierzenie stanowiska komputerowego lub innego sprzętu elektronicznego lub ich zdanie jest potwierdzane protokołem odbioru sprzętu. Protokół jest przechowywany przez ASI. Użytkownik sprzętu/aktywa może otrzymać kserokopię lub skan protokołu.
Nr 4.3	**Postępowanie z nośnikami** 4.3.1. Użytkownik systemu informatycznego odpowiada za posiadane nośniki (np. CD, DVD, Pendrive, dyski zewnętrzne, karty pamięci). ASI udziela niezbędnego wsparcia w zakresie stosowania technik kryptograficznych w przypadku, gdy Użytkownik systemu informatycznego zapisuje na nośnikach Dane Osobowe lub dane wrażliwe. 4.3.2. Nie należy przechowywać zbędnych nośników informacji zawierających dane chronione oraz kopii zapasowych, a także wydruków i innych dokumentów zawierających dane. Po upływie okresu ich użyteczności lub przechowywania, dane powinny zostać skasowane lub zniszczone tak, aby nie było możliwe ich odczytanie. 4.3.3. Nośniki wymienne/zewnętrzne (CD, DVD, pendrive, dyski, nośniki USB, karty pamięci i inne) wycofane z eksploatacji są niszczone w niszczarce lub przekazywane do zniszczenia zewnętrznemu podmiotowi. 4.3.4. Nośniki wymienne/zewnętrzne (np. pendrive, dyski, nośniki USB, karty pamięci i inne) wycofane z eksploatacji powinny być do czasu zniszczenia składowane w bezpiecznym miejscu (np. sejf, szafa zamykana na klucz) i dostępne tylko osobom upoważnionym przez ASI. Nośniki te można zniszczyć samodzielnie za pomocą specjalistycznego sprzętu lub przez zewnętrznego dostawcę. Zniszczenie nośników wymiennych jest dokumentowane *Protokołem zniszczenia nośników (Załącznik III.E.2-F1).* 4.3.5. W przypadku konieczności przekazania sprzętu komputerowego do naprawy serwisantowi zewnętrznemu należy wcześniej wymontować nośniki (dyski twarde) i przechować je na czas przeprowadzania naprawy sprzętu. Jeżeli naprawa nie jest możliwa bez demontażu nośnika, dostawca powinien przeprowadzić naprawę po podpisaniu umowy o zachowaniu poufności lub w siedzibie Organizacja (pod bezpośrednim nadzorem ASI lub upoważnionego przez niego pracownika Działu IT). 4.3.6. W przypadku odzyskiwania danych chronionych dopuszcza się przekazanie nośnika lub urządzenia z nośnikiem podmiotowi zewnętrznemu pod warunkiem uprzedniego podpisania umowy o zachowaniu poufności, a w sytuacji, gdy na nośniku znajdują się Dane Osobowe – Umowy o powierzeniu przetwarzania Danych Osobowych. Z przeprowadzonych prac sporządza się protokół zawierający co najmniej informacje: imię, nazwisko oraz podpis pracownika zewnętrznego, imię i nazwisko oraz podpis osoby nadzorującej prace, zakres przeprowadzenia prac oraz podstawę ich przeprowadzenia np. umowa, data rozpoczęcia i zakończenia prac, uwagi. 4.3.7. ASI (po konsultacji z przełożonym danej Jednostki Organizacyjnej) może wskazać stanowiska komputerowe, na których należy zablokować możliwość podłączania nośników zewnętrznych. Odblokowanie możliwości podłączania następuje zgodnie z zasadami kontroli dostępu. 4.3.8. Dokumentacja papierowa niszczona jest w niszczarkach paskowych oraz tam, gdzie to wymagane w niszczarkach o podwyższonym standardzie. 4.3.9. Dopuszcza się zlecenie zniszczenia dokumentacji papierowej przez specjalistyczną firmę. W takim przypadku firma ta zobowiązana jest do wykazania się bezpieczną procedurą utylizacji (np. posiadać certyfikat ISO27001, zapewniać nagrania z procesu transportu i utylizacji).
Nr 4.4	**Kontrola dostępu** 4.4.1. Dostęp do systemów operacyjnych, aplikacji oraz baz danych jest przydzielany przez ASI lub dostawców oprogramowania. Zobowiązani są oni (w miarę możliwości technicznych) do utworzenia kont awaryjnych („emergency") i umieszczenia haseł do takich kont w bezpiecznym miejscu wskazanym przez ASI. Hasła dla Użytkowników systemu informatycznego należy utworzyć zgodnie z zasadami określonymi w *Procedurze III.E.4 Regulamin Użytkownika systemów informatycznych.* 4.4.2. Dostęp jest przydzielany na wniosek przełożonego lub na wniosek Użytkownika systemu informatycznego (po potwierdzeniu zasadności przez przełożonego). Wnioski i potwierdzenia są dokumentowane elektronicznie. 4.4.3. Zmiany uprawnień w systemach operacyjnych, aplikacjach, usługach aplikacyjnych oraz bazach danych są wykonywane przez administratorów systemów na wniosek przełożonego lub na wniosek Użytkownika systemu (po potwierdzeniu przez przełożonego). Wnioski i potwierdzenia są dokumentowane elektronicznie. W przypadku, gdy zmiana uprawnień wiąże się ze zmianą zakresu dostępu do Danych Osobowych, administrator zwraca się do Koordynatora ds. ODO, który zgodnie z *Procedurą III.E.1 Polityka Ochrony Danych Osobowych* podejmuje działania w kierunku zmiany upoważnienia do przetwarzania Danych Osobowych (nadanego osobie, której dotyczy zmiana uprawnień). 4.4.4. Stosuje się następujące sposoby tworzenia identyfikatorów Użytkowników (login-ów): imię.nazwisko 4.4.5. Obowiązują następujące reguły tworzenia kont Użytkowników: a) należy unikać tworzenia i używania konta „gość",

	b) konta o uprawnieniach administracyjnych (root, administrator) powinny być przypisane tylko do faktycznych administratorów systemów (ASI i ewentualnie zewnętrzni serwisanci), c) konta wykorzystywane przez kilka osób (grupowe) mogą być stosowane jedynie w szczególnych przypadkach pod warunkiem wprowadzenia innych regulacji zapewniających rozliczalność działań wykonywanych przy pomocy takich kont; d) konta tymczasowe i „techniczne" mogą być stosowane wyłącznie do celów komunikacji i integracji między systemami. Użytkownicy nie mogą wykorzystywać tego typu kont do standardowego dostępu do systemów informatycznych lub takie wykorzystanie musi być monitorowane. 4.4.6. Nieużywane konta w systemach powinny być blokowane – należy unikać usuwania kont (aby zapewnić rozliczalność wymaganą przez RODO). Konta są blokowane na podstawie wniosku przełożonego w przypadku opuszczenia organizacji przez członka personelu. 4.4.7. Zaleca się wyłączanie bądź zmianę nazw kont administracyjnych wbudowanych w system. Zmiana haseł domyślnych takich kont jest obowiązkowa i powinna być wykonana przez ASI przed udostępnieniem systemu Użytkownikowi. 4.4.8. Uruchamianie usług bądź aplikacji w systemach należy wykonywać logując się na konto z uprawnieniami Użytkownika. Dopuszcza się stosowanie przez Użytkowników zatwierdzonych narzędzi tymczasowo podnoszących poziom uprawnień (np. tokenów). 4.4.9. ASI lub pracownicy Działu IT posiadający uprawnienia administracyjne do urządzeń serwerowych, urządzeń sieciowych, urządzeń przechowujących dane, baz danych i aplikacji oraz maszyn wirtualnych są zobowiązani do utworzenia na krytycznych urządzeniach kont „emergency". Dane uwierzytelniające do tego konta są umieszczane w bezpiecznym miejscu wskazanym przez ASI. 4.4.10. Systemy administrowane powinny spełniać wymagania w zakresie jakości haseł opisane w *Procedurze III.E.4 Regulamin Użytkownika systemów informatycznych.* 4.4.11. Przegląd kont i uprawnień w administrowanych systemach jest realizowany raz do roku. Przegląd ma na celu blokowanie nieużywanych kont oraz aktualizację uprawnień dla Użytkowników systemu informatycznego (w szczególności: ograniczanie niepotrzebnego dostępu dla Użytkowników).
Nr 4.5	**Stosowanie rozwiązań kryptograficznych** 4.5.1. ASI jest zobowiązany do stosowania zabezpieczeń kryptograficznych tam, gdzie jest to wykonalne i zasadne, w szczególności do: a) szyfrowania komunikacji podczas połączeń zdalnych (np. VPN, ssh), b) szyfrowania komunikacji w trakcie logowania do aplikacji i korzystania z nich z wykorzystaniem przeglądarki www (https), c) szyfrowania pamięci urządzeń mobilnych i przenośnych lub ich części (wolumeny), d) szyfrowania nośników zewnętrznych, e) zapisywania haseł w szyfrowanych repozytoriach, f) przesyłania wrażliwych informacji pocztą elektroniczną tylko w załącznikach zaszyfrowanych i zabezpieczonych hasłem. 4.5.2. ASI gromadzi informacje potrzebne do odzyskiwania zainstalowanych stanowisk komputerowych (np. klucze kryptograficzne). 4.5.3. Dla Użytkowników technologii kryptograficznych ASI udostępnia instrukcje obsługi (tam gdzie to uzasadnione). 4.5.4. Bezpieczeństwo wykorzystywanych rozwiązań kryptograficznych jest na bieżąco monitorowane przez ASI poprzez śledzenie informacji medialnych oraz przegląd stron www dostawców rozwiązań. W razie stwierdzenia ryzyka należy powiadomić Koordynatora ds. ODO.
Nr 4.6	**Dostęp do sprzętu i okablowania** 4.6.1. Sprzęt serwerowy, urządzenia sieciowe, urządzenia przechowywania danych, rejestratory do monitoringu są umieszczane w specjalnych pomieszczeniach (serwerownie, węzły dystrybucyjne i telekomunikacyjne) oraz w szafach na sprzęt (tzw. racki). 4.6.2. Dostęp do pomieszczeń w których znajduje się ww. urządzenia jest ograniczony do uprawnionych osób (ASI, pracownicy Działu IT). Szafy umieszczone w pomieszczeniach ogólnodostępnych są zamykane. 4.6.3. Osoby z zewnątrz wykonujące prace na rzecz organizacji (np. przeglądy i konserwacje sprzętu i systemów wspomagających, audyty, sprzątanie itp.) mogą przebywać w pomieszczeniach wyłącznie pod stałym nadzorem osób uprawnionych. 4.6.4. Pracownik nadzorujący dba o to, aby w pomieszczeniach przebywała jak najmniejsza ilość osób z zewnątrz jednocześnie. 4.6.5. Jeżeli nie jest możliwy stały nadzór nad osobami z zewnątrz, osoby te powinny być przeszkolone z zakresu zasad bezpieczeństwa obowiązujących w pomieszczeniach ze sprzętem przez personel nadzorujący prace. Wykonanie prac bez nadzoru musi być objęte umową zawierającą możliwość dochodzenia odszkodowania w przypadku naruszenia zasad bezpieczeństwa, umową w zakresie poufności oraz ewentualnie umową powierzenia Danych Osobowych. 4.6.6. Na terenie serwerowni obowiązuje bezwzględny zakaz stosowania ognia. 4.6.7. Na teren serwerowni nie wolno wnosić substancji stwarzających ryzyko dla sprzętu, np. płynów, napojów, pojemników z wodą, chemikaliów do czyszczenia powierzchni itp. 4.6.8. Warunki środowiskowe panujące w pomieszczeniach ze sprzętem powinny być monitorowane (w szczególności temperatura). 4.6.9. Sprzęt jest zabezpieczony przed przerwami lub zakłóceniami zasilania poprzez podtrzymanie napięcia (UPS). 4.6.10. Okablowanie powinno być ułożone w sposób zapobiegający przypadkowemu uszkodzeniu oraz w sposób utrudniający niezauważone podłączenie do nich. Przewody zasilające należy izolować od tych przesyłających dane. W uzasadnionych przypadkach zaleca się używanie przewodów w różnych kolorach (np. inny kolor dla podłączenia serwerów i inny kolor dla podłączenia urządzeń sieciowych) lub oznaczenie etykietami. 4.6.11. O czystość serwerowni, punktów dystrybucyjnych oraz innych pomieszczeń, w których znajdują się urządzenia teleinformatyczne (np. pojedyncze szafy) dbają pracownicy upoważnieni do przeprowadzania czynności porządkowych pod nadzorem pracownika MGGP S.A.

	4.6.12. ASI lub upoważnieni przez niego pracownicy Działu IT dokonują konserwacji sprzętu: a) gdy wymagają tego warunki gwarancji lub ubezpieczenia, b) przy okazji bieżącej pracy ze sprzętem, w przypadku podejrzenia nieprawidłowego funkcjonowania sprzętu z powodu zanieczyszczeń.
Nr 4.7	**Eksploatacja systemów** 4.7.1. ASI lub upoważnieni przez niego pracownicy Działu IT nadzorują na bieżąco wykorzystanie zasobów systemów (np. pamięci operacyjnej, obciążenia dysków i procesora, przepustowości sieci). Tam, gdzie to uzasadnione stosuje się narzędzia automatyzujące monitorowanie i zapewniające powiadomienie o zdefiniowanych zdarzeniach. 4.7.2. Wprowadzanie zmian w aktywach wspierających przetwarzanie informacji jest nadzorowane przez ASI, który identyfikuje zmiany standardowe (wynikające z bieżących aktualizacji). Wszelkie zmiany niestandardowe muszą być zarejestrowane. W przypadku zmian, które mogą mieć istotny wpływ na ochronę Danych Osobowych, ASI musi powiadomić Koordynatora ds. ODO w celu analizy zgodnie z *Procedurą III.E.1 Polityka Ochrony Danych Osobowych.* 4.7.3. Instalacja oprogramowania jest przeprowadzana według następujących zasad: a) **w systemach operacyjnych urządzeń sieciowych i serwerowych** instalację przeprowadza ASI lub upoważnieni przez niego pracownicy Działu IT. Administrator systemu jest zobowiązany uzyskać zgodę na wykorzystanie licencji przyznanej organizacji lub zweryfikować możliwość skorzystania z licencji ogólnej. Administrator systemu może wykorzystać listę licencji zweryfikowanych przez ASI; b) **w systemach operacyjnych stanowisk komputerowych** instalację przeprowadza ASI lub upoważnieni przez niego pracownicy Działu IT. Dla licencji przyznanych organizacji ASI jest zobowiązany wykorzystać licencję z posiadanej puli lub zweryfikować możliwość skorzystania z licencji ogólnej; c) **w systemach operacyjnych w urządzeniach przenośnych (tablety, smartfony)** instalację przeprowadza Użytkownik urządzenia (o ile posiada on prawa administracyjne). Użytkownik urządzenia jest zobowiązany uzyskać zgodę ASI na wykorzystanie licencji lub zweryfikować możliwość skorzystania z licencji ogólnej; 4.7.4. ASI jest odpowiedzialny za nadzór nad licencjami przydzielonymi indywidualnie. 4.7.5. Systemy operacyjne organizacji są chronione przez oprogramowanie antywirusowe instalowane przez ASI lub upoważnionych przez niego pracowników Działu IT. 4.7.6. ASI jest zobowiązany monitorować źródła informacji o zagrożeniach dla bezpieczeństwa Danych Osobowych związanych z eksploatacją systemów. W przypadku zidentyfikowania zagrożenia, które może wystąpić w organizacji, należy niezwłocznie zawiadomić Koordynatora ds. ODO w celu ustalenia postępowania (np. wydanie ostrzeżenia dla Użytkowników systemu informatycznego, szacowanie ryzyka).
Nr 4.8	**Przeglądy i konserwacje** 4.8.1. ASI lub upoważni przez niego pracownicy Działu IT prowadzą okresowe przeglądy systemów informatycznych w celu określania ich poziomu sprawności, biorąc pod uwagę racjonalne wykorzystanie sprzętu oraz bezpieczeństwo Danych przetwarzanych z jego wykorzystaniem. 4.8.2. Przeglądy i konserwacje sprzętu komputerowego oraz nośników informacji służących do przetwarzania Danych Osobowych i innych danych mających wartość dla Organizacji, przeprowadzane są w pomieszczeniach stanowiących obszar przetwarzania Danych, przez ASI lub upoważnieni przez niego pracownicy Działu IT. W umowach z podmiotami świadczącymi powyżej wskazane usługi powinno znajdować się postanowienie o powierzeniu Danych Osobowych i innych danych mających wartość dla Organizacji. W przypadku przekazywania do naprawy sprzętu komputerowego z zainstalowanym systemem informatycznym służącym do przetwarzania Danych Osobowych i innych danych mających wartość dla Organizacji lub nośnikiem informacji służących do przetwarzania Danych Osobowych i innych danych mających wartość dla Organizacji, należy postępować zgodnie z zasadami opisanymi w pkt. 4.3. 4.8.3. W przypadku konieczności dokonania naprawy elementu infrastruktury systemu informatycznego przez osobę nieupoważnioną (np. zewnętrzny serwis informatyczny) w obszarze przetwarzania Danych osobowych i innych danych istotnych dla Organizacji, wszelkie czynności dokonywane są pod bezpośrednim nadzorem ASI lub upoważnionych przez niego pracowników Działu IT. 4.8.4. ASI lub upoważnieni przez niego pracownicy Działu IT przeprowadzają przegląd okresowy, o którym mowa w pkt. 4.8.1 nie rzadziej niż raz na 6 miesięcy. 4.8.5. Nadzór nad przeprowadzaniem przeglądów technicznych, konserwacji i napraw sprzętu komputerowego, na którym zainstalowano system informatyczny służący do przetwarzania Danych Osobowych i innych danych mających wartość dla Organizacji, systemu informatycznego służącego do przetwarzania Danych Osobowych i innych danych istotnych dla Organizacji oraz nośników informacji służących do przetwarzania Danych Osobowych i innych danych istotnych dla Organizacji pełni ASI lub upoważnieni przez niego pracownicy Działu IT.
Nr 4.9	**Kopie zapasowe** 4.9.1. Kopie zapasowe powinny być kontrolowane przez ASI lub upoważnionych przez niego pracowników Działu IT, w szczególności pod kątem prawidłowości ich wykonania poprzez częściowe lub całkowite odtworzenie. 4.9.2. W przypadku likwidacji nośników informatycznych zawierających Dane Osobowe i inne dane istotne dla Organizacji lub kopie zapasowe systemów informatycznych służących do przetwarzania Danych Osobowych i innych danych istotnych dla Organizacji należy postępować zgodnie z zasadami opisanymi w pkt. 4.3.5. 4.9.3. Nośniki informatyczne zawierające Dane Osobowe i inne dane istotne dla Organizacji lub kopie systemów informatycznych służących do przetwarzania Danych Osobowych i innych danych istotnych dla Organizacji są przechowywane w sposób uniemożliwiający ich utratę, uszkodzenie lub dostęp osób nieuprawnionych. 4.9.4. W systemach informatycznych zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii Danych przetwarzanych przy użyciu systemów informatycznych. 4.9.5. Kopie zapasowe zbioru Danych Osobowych i innych danych istotnych dla Organizacji przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym Dane Osobowe i inne dane istotne dla Organizacji przetwarzane są na bieżąco.

	4.9.6. Kopie zapasowe serwera (z zawartością plików i baz danych) tworzone są w sposób zautomatyzowany w oparciu o specjalne oprogramowanie/skrypt/wykorzystanie programowej funkcji serwera. 4.9.7. Kopie sporządzane są na: streamerze, przenośnym dysku HDD / pendrive / wydzielonym serwerze NAS. 4.9.8. Kopie sporządzane są okresowo. 4.9.9. Przenośny dysk HDD / Pendrive przechowywany jest w oddziałach MGGP S.A. w zamykanych metalowych szafach. 4.9.10. Dostęp do przenośnego dysku HDD / pendrive / wydzielonego serwera NAS, streamerów ma ASI i uprawnieni przez niego pracownicy Działu IT. 4.9.11. ASI sprawuje nadzór nad poprawnością wykonania w/w kopii zapasowych.
Nr 4.10	**Zarządzanie siecią** 4.10.1. Bezpieczeństwo sieci jest zapewniane przez ASI poprzez stosowanie następujących mechanizmów ochrony: a) redundancja (nadmiarowość) łącz do sieci zewnętrznych, b) podział sieci poprzez fizyczne wydzielenie podsieci, zastosowanie sieci VLAN oraz ustanowienie sieci o specjalnych przeznaczeniach (sieć użytkowników, sieć dla systemów dostępnych publicznie, sieć dla systemów), c) zarządzanie urządzeniami poprzez komunikację szyfrowaną, bezpośrednie podłączenie kablowe lub dedykowane oprogramowanie, d) blokowanie stron www stwarzających zagrożenie dla bezpieczeństwa informacji, e) wyznaczenie w uzasadnionych przypadkach (np. sale konferencyjne) gniazd lub sieci WIFI z dostępem wyłącznie do Internetu, z których mogą korzystać osoby spoza MGGP S.A., f) okresowa zmiana haseł do sieci WIFI: • autoryzacja w sieci Wifi dla pracowników odbywa się poprzez mechanizm SSO zintegrowany z Microsoft AD, • dostęp WIFI dla gości realizowany jest poprzez ticketowy system haseł.
Nr 4.11	**Zarządzanie rozwojem systemów i aplikacji** 4.11.1. Reguły bezpieczeństwa zarządzania rozwojem systemów i aplikacji określone zostały w *Polityce bezpieczeństwa w rozwoju systemów i aplikacji (Załącznik III.E.2-Z1)*.
Nr 4.12	**Zdarzenia i incydenty bezpieczeństwa informacji** 4.12.1. Zdarzenia dotyczące bezpieczeństwa informacji mogą być zgłaszane ASI przez Użytkowników (w systemie Axence nVision) lub stwierdzane bezpośrednio przez ASI (np. podczas przeglądu logów). ASI jest odpowiedzialny za dokumentowanie i analizę zgłoszeń pod względem skutków dla bezpieczeństwa informacji (tj. czy wystąpiło naruszenie lub czy pojawiło się jakieś ryzyko naruszenia). 4.12.2. W przypadku wystąpienia incydentu w zakresie bezpieczeństwa Danych Osobowych ASI jest zobowiązany niezwłocznie powiadomić Koordynatora ds. ODO w celu dalszej analizy.
Nr 4.13	**Wyjątki** 4.13.1. Wyjątki od stosowania zasad opisanych w niniejszym dokumencie muszą być zgłaszane do Koordynatora ds. ODO, który identyfikuje ryzyka wynikającego z odstępstwa.
5. DOKUMENTY WZORCOWE / FORMULARZE I ICH UŻYKOWNICY	III.E.2-F1 – Protokół zniszczenia nośników – *ASI*
6. ZAŁĄCZNIKI	III.E.2-Z1 – Polityka bezpieczeństwa w rozwoju systemów i aplikacji

Procedura III.E.4 Regulamin Użytkownika systemów informatycznych

Właściciel procesu: Administrator Systemów Informatycznych			
Wersja: 03	Kategoria jawności: II (wewnętrzne)	Obowiązuje od: 01.02.2024 r.	Stron: 8

1. CEL I PRZEDMIOT PROCEDURY	Celem dokumentu jest zapewnienie odpowiedniej realizacji polityk bezpieczeństwa przez Personel MGGP S.A. obejmujący Użytkowników systemów informatycznych i/lub osoby upoważnione do przetwarzania danych osobowych i innych danych mających wartość dla Organizacji.
2. UCZESTNICY I ROLE W PROCEDURZE	**Personel, w tym Użytkownicy systemu informatycznego i/lub osoby upoważnione do przetwarzania danych osobowych:** - jest zobowiązany do przestrzegania zasad opisanych w niniejszej procedurze tj.: zasady czystego ekranu i pulpitu, zamkniętego pomieszczenia, czystego biurka, czystej tablicy, czystych drukarek, czystego kosza, zasady rozpoczęcia, zawieszenia i zakończenia pracy na komputerze lub w systemie informatycznym, polityki bezpieczeństwa haseł, zasad bezpiecznego użytkowania sprzętu IT, korzystania z urządzeń mobilnych, zasad korzystania z urządzeń prywatnych, korzystania z nośników elektronicznych, zasad dotyczących pracy zdalnej (na odległość) i pracy w miejscach publicznych, zasad korzystania z oprogramowania, Internetu, poczty elektronicznej, zasad aktualizacji oprogramowania i ochrony antywirusowej, zasad postępowania z informacjami w wersji papierowej, - w przypadku pozyskania wiedzy o naruszeniu Danych Osobowych podejmuje określone w procedurze działania i niezwłocznie powiadamia Koordynatora ds. ODO oraz bezpośredniego przełożonego, - obowiązany jest do przestrzegania zasad zachowania poufności dotyczących Danych Osobowych i innych danych mających wartość dla Organizacji oraz zasad dotyczących ich udostępniania, - jest zobowiązany do dbałości o powierzony mu przez MGGP S.A. sprzęt i ponosi pełną odpowiedzialność za jego utratę lub uszkodzenie.
3. TERMINOLOGIA	Definicje stosowane w niniejszym dokumencie zawarte są w słowniku.
4. INSTRUKCJE POSTĘPOWANIA	
Nr 4.1	**Procedura rozpoczęcia, zawieszenia i zakończenia pracy** 1.1.1. Użytkownik systemu informatycznego rozpoczyna pracę na komputerze lub w systemie informatycznym z użyciem identyfikatora (login) i hasła, które nie mogą być udostępnianie innym Użytkownikom systemu informatycznego. 1.1.2. Użytkownik systemu informatycznego jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, nieupoważnionym pracownikom) wglądu do danych wyświetlanych na monitorach komputerowych. Użytkownika systemu informatycznego obowiązuje tzw. Polityka czystego ekranu (pkt 4.3). 1.1.3. Przed opuszczeniem stanowiska pracy, Użytkownik systemu informatycznego zobowiązany jest uruchomić blokadę ekranu, wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu. 1.1.4. Przed przerwaniem pracy w systemie informatycznym i tymczasowym odejściem od punktu dostępowego i/lub po zakończeniu pracy, Użytkownik systemu informatycznego zobowiązany jest: a) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy (wyjątkiem są komputery wymagające pozostawienia w trybie pracy, w takim przypadku obowiązuje wylogowanie), b) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki elektroniczne, na których znajdują się dane wymagające ochrony (np. Dane Osobowe, dane klienta itd.). 1.1.5. Po zakończeniu pracy w systemie informatycznym Użytkownik systemu informatycznego zamyka system informatyczny, do którego ma dostęp. 1.1.6. Przed rozpoczęciem przetwarzania Danych Użytkownik systemu informatycznego powinien sprawdzić, czy nie ma oznak fizycznego naruszenia zabezpieczeń. W przypadku wystąpienia jakichkolwiek nieprawidłowości przetwarzania danych osobowych i innych danych mających wartość dla Organizacji, należy powiadomić Koordynatora ds. ODO i ASI. 1.1.7. Przed rozpoczęciem pracy w systemie informatycznym Użytkownik systemu informatycznego weryfikuje bezpieczeństwo treści wyświetlanych na ekranie ze względu na przebywanie osób nieupoważnionych w obszarze przetwarzania.
Nr 4.2	**Polityka bezpieczeństwa haseł** 4.2.1. W zależności od konkretnego systemu lub aplikacji, hasła do systemów informatycznych mogą być: a) ustalane przez komórkę organizacyjną odpowiedzialną za system (ASI lub Dział IT), b) wymuszane przez system, c) zmieniane przez Użytkownika systemu informatycznego (który musi pamiętać o okresowej zmianie hasła). 4.2.2. Użytkownik systemu informatycznego jest zobowiązany do zachowania poufności hasła, nawet po utracie przez nie ważności. 4.2.3. Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom. 4.2.4. Szczegółowe reguły dotyczące przyznawania dostępu oraz ustalania i zmiany haseł: a) pierwsze (pierwotne) hasło Użytkownika systemu informatycznego nadawane jest przez ASI lub upoważnionych przez niego pracowników Działu IT i przekazywane Użytkownikowi systemu informatycznego w poufny sposób, b) hasła administracyjne zdeponowane są w Dziale IT, dostęp do haseł posiadają uprawnieni pracownicy Działu IT, c) przypadku utraty uprawnień przez ASI należy niezwłocznie zmienić wszystkie hasła, do których miał dostęp (np. hasła administratorów, Użytkowników systemów informatycznych, urządzeń, dostępu do pomieszczeń, itp.), d) w sytuacjach awaryjnych (np. nieobecność ASI) hasło może być przekazane decyzją ADO osobie zastępującej ASI,

	e) o ustaniu sytuacji awaryjnej, ASI jest zobowiązany do zmiany haseł administracyjnych oraz tych, do których osoba zastępująca mogła uzyskać dostęp podczas zastępstwa, f) hasło zastosowane do uwierzytelnienia Użytkownika systemu informatycznego w systemie informatycznym składa się z określonej liczby znaków (co najmniej 12), w tym musi zawierać małe i duże litery oraz liczbę i znak specjalny. Hasło jest zmieniane w cyklach nie dłuższych niż 30 dni, g) hasło nie może składać się z danych personalnych (tj. imion, nazwisk, adresów zamieszkania użytkownika, jak również najbliższych dla niego osób) lub ich fragmentów, h) hasło nie może składać się z identycznych znaków lub ciągu znaków z klawiatury, i) hasło nie może być tożsame z identyfikatorem Użytkownika systemu informatycznego, j) hasło musi być za każdym razem nowe, tzn. takie, które nie było poprzednio stosowane przez Użytkownika systemu informatycznego, system pamięta 6 haseł wstecz, k) zmiana hasła dokonywana jest przez Użytkownika systemu informatycznego manualnie, l) hasło do uwierzytelnienia kont administracyjnych w systemach informatycznych składa się z określonej liczby znaków, w tym musi zawierać małe i duże litery oraz liczbę i znak specjalny, m) hasło w trakcie wpisywania, nie może być wyświetlane na ekranie, n) w przypadku złamania zasady poufności hasła, Użytkownik systemu informatycznego zobowiązany jest niezwłocznie zmienić hasło i poinformować o tym fakcie ASI, o) identyfikator Użytkownika systemu informatycznego nie powinien być zmieniany, a po wyrejestrowaniu Użytkownika z systemu informatycznego służącego do Przetwarzania Danych nie powinien być przydzielany innej osobie, p) identyfikator Użytkownika, który utracił uprawnienia do Przetwarzania Danych, należy niezwłocznie zablokować w systemie informatycznym służącym do Przetwarzania Danych oraz unieważnić przypisane mu hasło, q) Użytkownicy systemów informatycznych są zapoznawani z zagrożeniami wynikającymi ze stosowania haseł jako formy ich uwierzytelniania w systemie informatycznym, r) niedozwolone jest wykonywanie jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania Danych Osobowych z wykorzystaniem identyfikatora i hasła dostępu innego Użytkownika systemu informatycznego.
Nr 4.3	**Polityka czystego biurka i czystego ekranu** 4.3.1. Personel zobowiązany jest do przestrzegania następujących zasad: a) Zasada czystego ekranu i pulpitu, b) Zasada zamkniętego pomieszczenia, c) Zasada czystego biurka, d) Zasada czystej tablicy, e) Zasada czystych drukarek, f) Zasada czystego kosza. 4.3.2. Zasada czystego ekranu i pulpitu. a) Monitory komputerów, na których przetwarzane są wrażliwie dane (w tym Dane Osobowe), ustawione powinny być w sposób uniemożliwiający wgląd osobom nieupoważnionym, w szczególności nie będą skierowane w stronę okien lub przeszklonych drzwi i ścian. b) Przed pozostawieniem włączonego komputera bez opieki Użytkownicy systemu informatycznego powinni zapewnić by na ekranie nie były wyświetlane informacje, w tym Dane Osobowe, a w szczególności włączyć wygaszacz ekranu lub w przypadku dłuższej nieobecności wylogować się z systemu. c) Każdy komputer musi mieć ustawiony wygaszasz ekranu włączający się automatycznie po określonym czasie bezczynności Użytkownika systemu informatycznego nie dłuższym niż 5 minut. d) W przypadku wznowienia aktywności przez Użytkownika systemu informatycznego, wygaszacz powinien być wyłączany jedynie po podaniu hasła. e) Na pulpicie komputera mogą znajdować się jedynie ikony standardowego oprogramowania i aplikacji służbowych oraz skróty folderów pod warunkiem, że w nazwie nie zawierają Danych Osobowych. f) Wszelkie istotne dane i wyniki pracy powinny być przechowywane lokalnie tylko w wyjątkowych sytuacjach. Zaleca się przechowywanie danych i wyników pracy na dedykowanych do tego celu dyskach sieciowych. g) Użytkownicy systemów informatycznych muszą szczególnie zwracać uwagę na sposób usuwania plików (z pulpitu lub z zasobów sieciowych). Pliki, które zawierają jakiekolwiek wrażliwe informacje nie mogą być zamieszczane na zasobach ogólnodostępnych (np. przestrzeń „Trash" na dyskach sieciowych). 4.3.3. Zasada zamkniętego pomieszczenia. a) Zasada zamkniętego pomieszczenia obowiązuje wyłącznie w przypadku pomieszczeń, w których przetwarzane są Dane Osobowe lub inne dane mających wartość dla Organizacji. Zasada nie dotyczy pomieszczeń ogólnie dostępnych i przeznaczonych do wspólnego użytku. b) Niedopuszczalne jest pozostawianie niezabezpieczonego miejsca pracy przez personel, zarówno w godzinach pracy, jak i po jej zakończeniu. c) Osoba opuszająca pomieszczenie jako ostatnia (czyli w sytuacji, gdy w pomieszczeniu nie pozostaje żaden inny Użytkownik), ma obowiązek zamknąć pomieszczenie na klucz lub, w przypadku, gdy pomieszczenie nie jest zamykane, w inny sposób zabezpieczyć wszelkie wrażliwe informacje i nośniki zawierające Dane Osobowe i inne dane mające wartość dla Organizacji, zgodnie z zasadą czystego biurka. d) Po zakończeniu dnia pracy, ostatnia wychodząca z pomieszczenia osoba jest zobowiązana zamknąć wszystkie okna i drzwi oraz zabezpieczyć klucze do pomieszczenia zgodnie z obowiązującymi Procedurami. 4.3.4. Zasada czystego biurka. a) Nie należy pozostawiać dokumentów i nośników na biurku bez nadzoru. b) Po zakończeniu wykonywania obowiązków należy uprzątnąć biurko z dokumentów papierowych oraz innych nośników mogących zawierać Dane Osobowe i inne dane mające wartość dla Organizacji. c) Dokumenty i nośniki Danych powinny być przechowywane pod nadzorem Użytkownika lub w zamykanych i w miarę możliwości ognioodpornych szafach.

Nr 4.3	d) Na biurku nie mogą znajdować się napoje w pojemnikach grożących rozlaniem płynu. 4.3.5. Zasada czystej tablicy. a) Po zakończeniu korzystania z tablic i innych współdzielonych ekranów należy niezwłocznie uprzątnąć wszystkie materiały oraz oczyścić tablice w miejscach wykonywania obowiązków przez personel. b) Dane Osobowe i inne dane mające wartość dla Organizacji uzyskane w wyniku przetwarzania na tablicach, współdzielonych ekranach i nośnikach należy przenieść do Systemu Informatycznego lub zbioru papierowego dedykowanego do przetwarzania tych Danych. 4.3.6. Zasada czystych drukarek. a) Drukowane dokumenty powinny być zabierane z drukarek przez Użytkownika systemu informatycznego niezwłocznie po ich wydrukowaniu. b) W przypadku nieudanej próby drukowania, Użytkownik systemu informatycznego powinien skontaktować się z osobą odpowiedzialną za poprawne funkcjonowanie urządzenia w celu ustalenia dalszego postępowania, w tym usunięcia informacji z pamięci drukarki. c) Drukarki i kserokopiarki nie powinny być ustawione w miejscach, do których dostęp mają osoby postronne. Jeżeli drukarka znajduje się w takim miejscu to wydruk z niej możliwy jest po autoryzacji poprzez PIN/kartę dostępu. Faks powinien być ustawiony przy stanowisku pracy osoby upoważnionej do odbierania wiadomości z faksu w pomieszczeniu, które jest zamykane poza normalnymi godzinami pracy. 4.3.7. Zasada czystego kosza. a) Dokumenty papierowe zawierające dane osobowe i inne dane mające wartość dla Organizacji powinny być niszczone za pomocą niszczarek w sposób uniemożliwiający odczytanie tych danych lub mogą być umieszczane w specjalnie przeznaczonych do tego pojemnikach (jeżeli niszczenie tych dokumentów zlecone jest podmiotom zewnętrznym). b) Powierzenie niszczenia dokumentów podmiotom zewnętrznym wymaga zgody Zarządu ADO i zawarcia Umowy Powierzenia.
Nr 4.4	**Ogólne zasady bezpiecznego użytkowania sprzętu IT** 4.4.1. Użytkownik otrzymuje sprzęt od ASI na podstawie zgłoszeń. Sprzęt jest odpowiednio zabezpieczony zgodnie z Procedurą zarządzania infrastrukturą IT. Minimalne wymagania to: a) dostęp do urządzenia jest zabezpieczony (np. hasło, kod PIN, blokada na podstawie linii papilarnych), b) nośnik danych na urządzeniu jest zaszyfrowany, c) urządzenie ma włączone automatyczne aktualizacje systemu operacyjnego, d) urządzenie ma zainstalowany program antywirusowy i włączone automatyczne aktualizacje bazy sygnatur wirusów, e) konto systemowe Użytkownika systemu informatycznego jest kontem o ograniczonych uprawnieniach. 4.4.2. Powierzenie sprzętu Użytkownikowi systemu informatycznego jest potwierdzane pisemnie. 4.4.3. Użytkownik systemu informatycznego jest odpowiedzialny za przydzielony sprzęt i jest zobowiązany korzystać ze sprzętu w sposób zgodny z jego przeznaczeniem oraz chronić go przed jakimkolwiek zniszczeniem lub uszkodzeniem. 4.4.4. Użytkownik systemu informatycznego zobowiązany jest do zabezpieczenia sprzętu IT przed dostępem osób nieupoważnionych oraz nie może wyłączać zabezpieczeń opisanych w punkcie 4.4.1. 4.4.5. Użytkownik systemu informatycznego ma obowiązek natychmiast zgłosić zagubienie, utratę lub zniszczenie powierzonego mu Sprzętu IT. 4.4.6. Samowolne otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione, chyba że ASI wyda każdorazowo takie zezwolenie i zostanie to odnotowane. 4.4.7. Użytkownik systemu informatycznego ma obowiązek zwrócić sprzęt oraz inne posiadane aktywa w razie ustania współpracy z organizacją.
Nr 4.5	**Zasady korzystania z urządzeń mobilnych** 4.5.1. Przydzielanie sprzętu indywidualnego. W przypadku przydzielenia sprzętów imiennie do Użytkownika systemu informatycznego, zobowiązany jest on do pokwitowania odbioru. W przypadku przekazania Użytkownikowi systemu informatycznego karty SIM, jest on informowany przez osobę odpowiedzialną za realizację umowy z operatorem o przysługującym limicie kosztów wykonywanych połączeń lub limicie transmisji danych. 4.5.2. Praca na urządzeniu mobilnym: a) Użytkownicy systemu informatycznego powinny korzystać z urządzeń mobilnych uwzględniając Politykę czystego ekranu oraz nie powinni wyłączać zabezpieczeń opisanych w punkcie 4.4.1 niniejszej Procedury, b) urządzenia mobilne mogą być wynoszone poza biura organizacji, c) zaleca się, aby dostęp do danych i aplikacji znajdujących się w urządzeniu mobilnym był odpowiednio zabezpieczony poprzez szyfrowanie danych, konieczność używania haseł itp., d) jeżeli jest to zasadne, Użytkownik systemu informatycznego powinien wykonywać kopie zapasowe informacji zawartych lokalnie w urządzeniach mobilnych, e) w przypadku utraty, w tym kradzieży lub zgubienia urządzenia przenośnego, Użytkownik systemu informatycznego powinien natychmiast powiadomić o tym ADO, ASI oraz Koordynatora ds. ODO zaznaczając jednocześnie, jakiego rodzaju dane były zapisane na utraconym urządzeniu, f) Użytkownik systemu informatycznego zobowiązany jest do zabezpieczenia urządzenia przenośnego w czasie transportu, a w szczególności: ▪ transport powinien odbywać się w torbie komputerowej, torbie, teczce lub aktówce, ▪ zabronione jest pozostawianie urządzenia przenośnego w samochodzie podczas postoju w miejscu publicznym bez nadzoru, ▪ podczas jazdy samochodem zabronione jest przewożenie urządzeń na siedzeniach. g) w przypadku, gdy urządzenie przenośne pozostawione jest w miejscu dostępnym dla osób nieupoważnionych, Użytkownik systemu informatycznego jest zobowiązany do stosowania linki zabezpieczającej, w szczególności dotyczy to zabezpieczenia komputera na stanowisku pracy, podczas konferencji, prezentacji, szkoleń, targów, itp.,

	h) w przypadku pozostawiania urządzenia przenośnego w pomieszczeniach biurowych zaleca się umieszczanie ich po zakończeniu pracy w zamykanych szafkach, i) pracując na urządzeniu przenośnym w miejscach publicznych i środkach transportu, Użytkownik systemu informatycznego zobowiązany jest chronić wyświetlane na monitorze/ekranie informacje przed wglądem osób nieupoważnionych. 4.5.3. Zdawanie sprzętu. Użytkownik sprzętu oddając sprzęt przekazany w użytkowanie zobowiązany jest do jego zwrócenia w stanie niepogorszonym wynikającym z jego normalnej eksploatacji.
Nr 4.6	**Zasady korzystania z urządzeń prywatnych** 4.6.1. Korzystanie z urządzeń prywatnych w celu realizacji działań zleconych przez MGGP S.A. jest dopuszczalne tylko w uzasadnionych przypadkach i tylko za zgodą ADO wyrażoną w formie dokumentowej. 4.6.2. Uzasadnione przypadki korzystania z urządzeń prywatnych to brak dostępnego sprzętu firmowego, nagła awaria sprzętu firmowego w podróży służbowej lub przy pracy zdalnej, lub podobne. 4.6.3. Użytkownicy powinni korzystać z urządzeń prywatnych uwzględniając Politykę czystego ekranu oraz powinni zapewnić, że urządzenie spełnia wymagania opisane w punkcie 4.4.1 niniejszej Procedury oraz inne zdefiniowane przez MGGP S.A.
Nr 4.7	**Zasady korzystania z nośników elektronicznych** 4.7.1. Informacje ogólne. a) Elektroniczne nośniki danych to m.in.: dyski zewnętrzne, pendrive, płyty CD/DVD, pamięci typu flash i inne. b) Użytkownik systemu informatycznego odpowiada za nośniki udostępnione mu przez organizację. c) Jeżeli nośnik został zabezpieczony przez ASI (np. poprzez szyfrowanie), Użytkownik systemu informatycznego ma zakaz wyłączania tych zabezpieczeń. d) W celu zachowania poufności Danych Osobowych i innych danych mających wartość dla Organizacji zabrania się stosowania nośników innych niż pochodzące od organizacji. e) Zabrania się pozostawiania nośników danych w sposób niezabezpieczony umożliwiający dostęp osobom nieupoważnionym. Nośniki powinny być objęte stałym nadzorem Użytkownika systemu informatycznego. 4.7.2. Wynoszenie nośników poza teren organizacji. a) Nośniki mogą być wynoszone z terenu firmy tylko na potrzeby wykonywanych obowiązków. b) Jeżeli wynoszony nośnik zawiera wrażliwe dane (np. dane osobowe) to należy te dane zaszyfrować. ASI udziela niezbędnego wsparcia w zakresie stosowania technik kryptograficznych w przypadku, gdy pracownik zapisuje dane osobowe lub dane wrażliwe.
Nr 4.8	**Zasady dotyczące pracy na odległość, w tym pracy w miejscach publicznych** 4.8.1. Praca na odległość ma miejsce, gdy Personel wykonuje swoją pracę zdalnie dla organizacji w miejscu znajdującym się poza terenem organizacji. Do miejsc takich zaliczają się: a) lokalizacje należące do Klientów, podwykonawców lub innych stron trzecich, b) miejsca publiczne, w których wykonywana jest praca lub odbywa się komunikacja (np. hotele, dworce, lotniska, restauracje, punkty z dostępem do hot-spot), c) prywatne miejsca zamieszkania osób wykonujących tam pracę na odległość. 4.8.2. Personel musi mieć upoważnienie do wykonywania pracy na odległość. Upoważnienie takie: a) może wynikać bezpośrednio z umowy, w której wpisano adres wykonywania pracy inny niż siedziba organizacji, lub b) może wynikać z rodzaju umowy (np. umowa o pracę zdalną), lub c) może być nadane w formie pisemnej, lub d) może wynikać z zarządzenia/uchwały ADO. 4.8.3. Do pracy na odległość może być wykorzystywany wyłącznie sprzęt będący własnością MGGP S.A. oraz sprzęt prywatny, ale tylko za zgodą ADO (pkt 4.6). 4.8.4. W przypadku, gdy Personel wykonuje swoją pracę zdalnie dla organizacji lub praca odbywa się w miejscu publicznym, ma on obowiązek odpowiednio wcześniej przeanalizować potencjalne zagrożenia oraz musi stosować się do zasad pracy na odległość. 4.8.5. Podczas pracy na odległość lub w miejscu publicznym należy szczególnie zwrócić uwagę na następujące sytuacje stanowiące zagrożenie dla bezpieczeństwa informacji i Danych Osobowych: a) pozostawianie aktywów bez opieki i narażenie na kradzież sprzętu, nośników lub dokumentów, b) używanie sprzętu, nośników lub dokumentów w miejscu lub w sposób narażający na uszkodzenie (np. zalanie, przegrzanie), c) pracę w położeniu ułatwiającym obserwowanie przez nieupoważnione osoby ekranu urządzenia lub klawiatury, d) pracę w miejscach publicznych, gdzie jest możliwa obecność urządzeń nagrywających obraz i/lub dźwięk, e) pracę w miejscach publicznych, gdzie jest możliwe podsłuchanie rozmowy przez osoby nieuprawnione, f) pracę z wykorzystaniem środków łączności narażających na połączenie się nieuprawnionej osoby z urządzeniem należącym do firmy (np. z komputerem, laptopem, tabletem, telefonem komórkowych) poprzez WIFI, LAN, Bluetooth, IRDA, itd. g) korzystanie przez nieuprawnione osoby ze sprzętu lub nośników (np. chwilowe użyczanie laptopa lub telefonu komórkowego, pożyczanie pendrive), h) nieuprawniony dostęp do informacji lub zasobów ze strony osób teoretycznie zaufanych, np. rodziny lub przyjaciół, i) pracę w miejscu narażającym na możliwość utraty danych przechowywanych na nośnikach w wyniku działania sił natury (zbyt wysoka lub zbyt niska temperatura, opady atmosferyczne, silne pola elektromagnetyczne), j) pracę z wykorzystaniem sprzętu lub nośników niebędących własnością firmy (możliwa obecność wirusów, keyloggerów itp.)

	4.8.6. Podczas pracy na odległość lub pracy w miejscu publicznym obowiązują następujące zasady: a) Należy bezwzględnie przestrzegać wymagań Polityki czystego biurka i Polityki czystego ekranu. b) Należy przestrzegać instrukcji producenta dotyczących właściwego użytkowania sprzętu w celu zapobieżenia jego uszkodzeniu (np. z powodu światła słonecznego, temperatury, wilgotności, opadów atmosferycznych, pola elektromagnetycznego itd.). a) Nie należy pozostawiać dokumentów, nośników danych i sprzętu w hotelach, w samochodzie, w domu itp. bez dodatkowego zabezpieczenia adekwatnego do ryzyka (sejf, linka zabezpieczająca, bagażnik z niewidoczną zawartością, szafka zamykana). b) Urządzenia przenośne oraz nośniki danych nie powinny być pozostawiane bez nadzoru w miejscach publicznych. c) Należy unikać korzystania z sieci domowych, hot-spotów lub innych punktów dostępu do Internetu, które nie spełniają wymagań organizacji. Należy korzystać wyłącznie z rozwiązań dostarczonych przez organizację (np. modemy, zawsze połączenia VPN). d) Należy unikać korzystania ze sprzętu lub nośników niebędących własnością organizacji. W szczególności obowiązuje całkowity zakaz drukowania dokumentów z informacjami chronionymi za pomocą urządzeń niebędących własnością organizacji. Wydruk dokumentów należy poprzedzić analizą ryzyka, a w razie potrzeby skonsultować z przełożonym lub Koordynatorem ODO. W przypadku korzystania ze sprzętu niebędącego własności organizacji na potrzeby dostępu do zasobów firmy należy przestrzegać postanowień Procedury kontroli dostępu. e) Należy unikać użyczania nieupoważnionym osobom sprzętu i nośników należących do organizacji. Ewentualny dostęp osób trzecich do sprzętu powinien być zapewniony na wydzielonym koncie lokalnym urządzenia z konfiguracją uniemożliwiającą na dostęp do zasobów organizacji. f) Rozmowy dotyczące informacji chronionych mogą być prowadzone tylko w bezpiecznych, sprawdzonych miejscach. Nie powinny się odbywać w obecności osób przypadkowych ani w miejscach nie zapewniających odpowiedniej ochrony takich jak: szkolenia, targi, restauracje, środki komunikacji publicznej itd. g) Podczas pracy w domu lub w podróży należy stosować dostępne zabezpieczenia (np. zamykanie sprzętu podczas nieużywania; zabezpieczenie dostępu do komputerów; nakładki ochronne na ekran; pozostawianie sprzętu w sposób zapobiegający upadkowi, zalaniu lub spaleniu). W czasie podróży należy przewozić nieużywane komputery przenośne w bagażu podręcznym i maskować je. Należy również uwzględnić zabezpieczenia wynikające z podpisanych polis ubezpieczeniowych dotyczących sprzętu. h) W przypadku form wymiany informacji takich jak komunikacja głosowa, wizyjna lub faksowa należy na miejscu ocenić ryzyko takiej wymiany. Rozmowa prowadzona w miejscu publicznym nie może zostać podsłuchana, wiadomości pozostawione na automatycznej sekretarce nie mogą być odsłuchane przez niepowołane osoby, a faksy nie mogą być przesłane przez pomyłkę do niewłaściwej osoby lub odebrane przez osobę nieposiadającą odpowiedniego upoważnienia.
Nr 4.9	**Zasady korzystania z oprogramowania** 4.9.1. Użytkownik systemu informatycznego zobowiązuje się do korzystania wyłącznie z oprogramowania dostarczonego wraz z urządzeniem lub zainstalowanego przez ASI lub upoważnionych przez niego pracowników Działu IT. 4.9.2. Użytkownik systemu informatycznego nie ma prawa kopiować oprogramowania zainstalowanego na Sprzęcie IT na swoje własne potrzeby ani na potrzeby osób trzecich. 4.9.3. Instalowanie jakiegokolwiek oprogramowania na Sprzęcie IT może być dokonane wyłącznie przez ASI lub lub upoważnionych przez niego pracowników Działu IT. 4.9.4. Użytkownicy systemu informatycznego nie mają prawa do instalowania ani używania oprogramowania innego, niż przekazane, udostępnione lub zaakceptowane przez organizację. Zakaz dotyczy między innymi instalacji oprogramowania z nośników danych, programów ściąganych ze stron internetowych, itp. 4.9.5. Użytkownicy systemu informatycznego nie mają prawa do zmiany konfiguracji oprogramowania, bez wcześniejszej konsultacji z ASI lub z upoważnionymi przez niego pracownikami Działu IT. 4.9.6. W przypadku naruszenia któregokolwiek z powyższych postanowień organizacja ma prawo niezwłocznie i bez uprzedzenia usunąć nielegalne lub niewłaściwie zainstalowane oprogramowanie.
Nr 4.10	**Zasady korzystania z Internetu** 4.10.1. Użytkownicy systemu informatycznego mają prawo korzystać z Internetu w celu wykonywania obowiązków służbowych. 4.10.2. Przy korzystaniu z Internetu, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i praw autorskich. 4.10.3. Użytkownicy systemu informatycznego mają prawo korzystać z Internetu dla celów prywatnych wyłącznie okazjonalnie i powinno być ono ograniczone do niezbędnego minimum. 4.10.4. Korzystanie z Internetu dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych, a także na wydajność systemu informatycznego organizacji. 4.10.5. Użytkownicy systemu informatycznego mają zakaz przeglądania w Internecie treści łamiących prawo lub mogących narazić organizację na konsekwencje prawne lub wizerunkowe. Zabrania się także grać w gry komputerowe w Internecie oraz ściągać z Internetu pliki niezwiązane z obowiązkami służbowymi. 4.10.6. W zakresie dozwolonym przepisami prawa, organizacja zastrzega sobie prawo kontrolowania sposobu korzystania przez Użytkownika systemu informatycznego z Internetu pod kątem wyżej opisanych zasad. Ponadto, w uzasadnionym zakresie, organizacja zastrzega sobie prawo kontroli czasu spędzanego przez Użytkownika systemu informatycznego w Internecie. Pracodawca może również blokować dostęp do niektórych treści dostępnych przez Internet. 4.10.7. Użytkownicy systemu informatycznego mają zakaz zapisywania plików zawierających informacje służbowe lub Dane Osobowe poza systemami udostępnionymi przez organizację. W szczególności zabrania się zapisywać ww. pliki na prywatnych kontach w serwisach chmurowych (typu: Dropbox, Google Drive, OneDrive itp.) lub wysyłania tych plików na prywatną pocztę e-mailową.

Nr 4.11	**Zasady korzystania z poczty elektronicznej** 4.11.1. System poczty elektronicznej jest przeznaczony wyłącznie do wykonywania obowiązków służbowych. 4.11.2. Użytkownicy systemu informatycznego mają prawo korzystać z Systemu poczty elektronicznej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum. 4.11.3. Korzystanie z Systemu Poczty Elektronicznej dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika systemu informatycznego pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych, a także na wydajność Systemu Poczty Elektronicznej. 4.11.4. Użytkownik systemu informatycznego jest świadomy, że wszelkie wiadomości o charakterze prywatnym utworzone lub odebrane za pośrednictwem Systemu poczty elektronicznej przetwarzane są wyłącznie na jego własną odpowiedzialność. Użytkownik systemu informatycznego wyraża zgodę na prowadzenie kontroli tych wiadomości przez Organizację. Organizacja nie będzie w tej sytuacji odpowiadać za przypadkowe naruszenie dóbr osobistych Użytkownika w postaci naruszenia tajemnicy korespondencji. 4.11.5. Użytkownicy systemu informatycznego nie mają prawa korzystać z Systemu poczty elektronicznej w celu rozpowszechniania treści łamiących prawo lub mogących narazić organizację na konsekwencje prawne lub wizerunkowe. 4.11.6. Bez zgody przełożonego Użytkownik systemu informatycznego nie ma prawa wysyłać wiadomości zawierających informacje chronione dotyczące organizacji, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej. 4.11.7. Użytkownicy systemu informatycznego nie powinni otwierać maili, które niosą ryzyko dla bezpieczeństwa Danych Osobowych. W szczególności należy zachować ostrożność przy e-mailach: • których tytuł nie sugeruje związku z wypełnianymi przez Użytkownika obowiązkami służbowymi (np. reklamy, prośby o wypełnienie ankiety), • od nieznanych nadawców, • zawierających żądania logowania się do programów lub serwisów internetowych, • zawierających pliki, o które Użytkownik systemu informatycznego nigdy nie prosił. 4.11.8. Użytkownicy systemu informatycznego nie powinni uruchamiać wykonywalnych plików załączonych do wiadomości przesyłanych pocztą elektroniczną (zazwyczaj są to pliki excel lub pliki MS Office zawierające makra). W sytuacji otrzymania takiego pliku lub przypadkowego uruchomienia go – Użytkownik systemu informatycznego ma obowiązek niezwłocznie powiadomić o tym ASI. 4.11.9. W przypadku konieczności przesyłania plików zawierających Dane Osobowe, Użytkownik systemu informatycznego zobowiązany jest do odpowiedniego zabezpieczenia pliku (zaszyfrowanie) zgodnie z zaleceniami ASI. Hasło do zaszyfrowanego pliku należy przesłać do odbiorcy odrębnym kanałem (np. SMS-em). 4.11.10. Przy wysyłaniu e-maili do osób z poza organizacji zaleca się stosowanie rozwiązania UDW („ukryte do wiadomości") w celu zmniejszenia ryzyka ujawnienia Danych Osobowych odbiorców e-maila.
Nr 4.12	**Zasady aktualizacji oprogramowania i ochrony antywirusowej.** 4.12.1. Użytkownicy systemu informatycznego zobowiązani są do niezwłocznego poinformowania ASI lub upoważnionych przez niego pracowników Działu IT o każdym przypadku powiadomienia o konieczności aktualizacji oprogramowania. 4.12.2. Użytkownicy systemu informatycznego zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym. 4.12.3. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego. 4.12.4. W przypadku stwierdzenia zainfekowania systemu, Użytkownik systemu informatycznego obowiązany jest poinformować niezwłocznie o tym fakcie ASI lub swojego przełożonego. 4.12.5. Użytkownicy systemu informatycznego zobowiązani są do regularnych aktualizacji bazy sygnatur wirusów. Zakazane jest nieuzasadnione przerywanie procesu aktualizacji. Aktualizacje powinny być uruchamiane bez zbędnej zwłoki.
Nr 4.13	**Zasady bezpieczeństwa dla Członków Personelu współpracujących z ADO na podstawie innych stosunków prawnych (niż umowa o pracę).** 4.13.1. Personel realizujący umowy zawarte z ADO na sprzęcie komputerowym będącym własnością ADO jest traktowany jak użytkownik systemu informatycznego, w związku z czym obowiązany jest do: a) odbycia szkoleń dedykowanych z zakresu bezpieczeństwa informacji i RODO udostępnionych przez ADO, b) zapoznania się z procedurami ADO z zakresu bezpieczeństwa informacji i RODO oraz podpisania stosownego oświadczenia – formularz III.E.4-F1 *Oświadczenie członka personelu MGGP S.A.*, które stanowi załącznik do umowy. 4.13.1. Dostawcy wykonujący umowy zawarte z ADO, do których nie stosuje się pkt 4.13.1 zobowiązani są przed zawarciem umowy: a) wypełnić formularz III.E.4-F2 Ankieta zgodności Dostawcy z wymaganiami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (RODO) oraz Procedurami MGGP S.A. w obszarze bezpieczeństwa informacji oraz do zapoznania się z zasadami bezpieczeństwa informacji, b) zapoznania się z zasadami bezpieczeństwa informacji (Załącznik III.E.4-Z1). Obydwa ww. dokumenty stanowią załącznik do umowy pomiędzy Wykonawcą a ADO. W razie stwierdzenia potrzeby, Administrator może zobowiązać Dostawcę do zawarcia porozumienia w przedmiocie korzystania ze sprzętu nie będącego własnością MGGP S.A. – formularz III.E.4-F1 *Porozumienie w sprawie używania sprzętu niebędącego własnością MGGP S.A.*, a także odbycia szkoleń, udostępnionych przez Administratora, w zakresie bezpieczeństwa informacji oraz ochrony danych osobowych, zwiększających świadomość na temat potencjalnych zagrożeń i możliwości ich unikania.
Nr 4.14	**Zasady postępowania z informacjami w wersji papierowej** Zasady postępowania z informacjami w wersji papierowej szczegółowo opisuje Załącznik III.E.1-Z1 do procedury III.E.1 Polityka Ochrony Danych Osobowych.

Nr 4.15	**Zgłaszanie incydentów (naruszeń)** 4.15.1 Jako incydent określa się zbiór złożony z jednego lub więcej zdarzeń lub uwarunkowań związanych z naruszeniem lub podejrzeniem naruszenia bezpieczeństwa informacji, w tym w szczególności ochrony Danych Osobowych (Naruszenie ODO), wymagający podjęcia działania i rozwiązania powstałego problemu w celu utrzymania akceptowalnego poziomu ryzyka. 4.15.2 Najczęstszymi obszarami i przykładami incydentów, z których każdy składa się z jednego lub więcej zdarzeń jest: a) utrata aktywów lub dostępu do usługi np. kradzież lub zagubienie nośnika danych, laptopa, karty dostępu lub kluczy, b) niewłaściwe działanie systemu informatycznego lub jego przeciążenie, c) niezgodność z wytycznymi lub procedurą bezpieczeństwa np. niestosowanie ustalonych zasad nadawania i zmiany haseł, d) naruszenie bezpieczeństwa fizycznego np. przebywanie nieuprawnionej osoby w pomieszczeniu chronionym, e) zainfekowanie systemu informatycznego na dużą skalę przez wirusy komputerowe itp., f) Wykorzystanie sprzętu IT przez Użytkownika systemu informatycznego w niewłaściwych celach, g) Próby włamania się do komputera (udane lub nieudane) w celu uzyskania nieautoryzowanego dostępu do systemu lub jego danych, h) Niekontrolowane zmiany i modyfikacje systemu – np. wprowadzenie zmian w sprzęcie lub oprogramowaniu bez wiedzy, zgody czy odpowiednich wskazówek od ASI. 4.15.3 W przypadku faktycznego lub potencjalnego naruszenia Danych Osobowych, każda osoba, która dowiedziała się, że mogło lub może dojść do takiego naruszenia, zobowiązany jest: **a)** powstrzymać się od rozpoczęcia lub od kontynuowania jakichkolwiek czynności mogących spowodować zatarcie śladów bądź dowodów związanych z danym Naruszeniem; **b)** podjąć niezbędne działania aby zapobiec eskalacji Naruszenia; **c)** podjąć niezbędne działania, aby zabezpieczyć te elementy systemu informatycznego, Zbioru Danych Osobowych lub samych danych, które na tym etapie nie zostały objęte Naruszeniem ODO; **d)** niezwłocznie, nie dłużej niż w ciągu 2 godzin, powiadomić Koordynatora ds. ODO o danym Naruszeniu ODO: • poprzez zgłoszenie w systemie Axence nVision, lub • przesyłając pocztą elektroniczną formularz, którego wzór zawarto w *Formularzu III.E.1-F7* w Polityce ochrony danych osobowych, lub • telefonicznie/osobiście; **e)** dodatkowo powiadomić bezpośredniego przełożonego w strukturze organizacyjnej.
Nr 4.16	**Zachowanie poufności** 4.16.1 Każda z osób dopuszczona do przetwarzania Danych Osobowych i innych danych mających wartość dla Organizacji jest zobowiązana do: a) przetwarzania Danych Osobowych i innych danych mających wartość dla Organizacji wyłącznie w zakresie i celu określonym w upoważnieniu, b) zachowania w tajemnicy Danych Osobowych i innych danych mających wartość dla Organizacji, do których ma dostęp w związku z wykonywaniem zadań, c) niewykorzystywania Danych Osobowych i innych danych mających wartość dla Organizacji w celach niezgodnych z zakresem i celem określonym w upoważnieniu, d) zachowania w tajemnicy sposobów zabezpieczenia Danych Osobowych, innych danych mających wartość dla Organizacji i systemów informatycznych przetwarzających te dane, e) ochrony Danych Osobowych i innych danych mających wartość dla Organizacji przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją Danych Osobowych i innych danych mających wartość dla Organizacji, nieuprawnionym ujawnieniem Danych Osobowych i innych danych mających wartość dla Organizacji, nieuprawnionym dostępem do Danych Osobowych i innych danych mających wartość dla Organizacji oraz przetwarzaniem. 4.16.2 Jeśli jest to przewidziane, osoba dopuszczona do przetwarzania odbywa szkolenie z zasad ochrony Danych Osobowych i innych danych mających wartość dla Organizacji. 4.16.3 Zabrania się przekazywania lub ujawniania Danych Osobowych i innych danych mających wartość dla Organizacji osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich Danych. 4.16.4 Zabrania się ujawniania na grupach dyskusyjnych, forach internetowych, blogach itp., jakichkolwiek szczegółów dotyczących funkcjonowania firmy, w tym informacji na temat sprzętu i oprogramowania, z jakiego korzysta firma, oraz informacji kontaktowych innych, niż ogólnodostępne w materiałach zewnętrznych. 4.16.5 Obowiązek zachowania poufności dotyczy także informacji stanowiących tajemnicę przedsiębiorstwa Organizacji oraz innych informacji poufnych. Personel mający dostęp do informacji stanowiących tajemnicę przedsiębiorstwa Organizacji oraz innych informacji poufnych jest zobowiązany do odpowiedniego przestrzegania zasad postępowania określonych powyżej.
Nr 4.17	**Udostępnianie Danych Osobowych i innych danych mających wartość dla Organizacji** 4.17.1 Osoba przetwarzająca Dane Osobowe i inne dane mające wartość dla Organizacji może udostępniać Dane drogą telefoniczną jedynie wtedy, gdy ma pewność co do tożsamości swojego rozmówcy (w razie wątpliwości należy weryfikować tożsamość np. poprzez żądanie podania fragmentu informacji znanej tylko osobie właściwej). 4.17.2 Dane Osobowe i inne dane mające wartość dla Organizacji można udostępnić tylko osobie, której dane dotyczą, lub innej osobie za jej zgodą przechowywaną w celach dowodowych przy zachowaniu procedury przewidzianej w ust. 1 powyżej. 4.17.3 Udostępniając Dane Osobowe i inne dane mające wartość dla Organizacji w miejscach publicznie dostępnych, należy zagwarantować poufność Danych. Jeżeli ustne przekazanie Danych nie gwarantuje poufności, należy skorzystać z udostępnienia w wersji pisemnej (do wglądu).

	4.17.4 Należy zwracać uwagę na sytuacje mogące stanowić ryzyko ujawnienia Danych Osobowych i innych danych mających wartość dla Organizacji lub informacji o stosowanych zabezpieczeniach osobie nieupoważnionej, takie jak: a) żądanie udostępnienia danych przez osoby podszywające się (kradzież tożsamości), b) żądanie udostępnienia informacji o stosowanych zabezpieczeniach, w tym w szczególności udostępnienia obecnych, jak i poprzednio stosowanych haseł dostępowych do systemów informatycznych (socjotechnika telefoniczna), c) wszelkie inne nieuzasadnione i podejrzane żądania udostępnienia informacji, w szczególności drogą telefoniczną.
Nr 4.18	**Postępowanie dyscyplinarne** 4.18.1 Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego Regulaminu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub umownych. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można podjąć odpowiednie kroki prawne. 4.18.2 Kara dyscyplinarna, orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez organizację o zrekompensowanie poniesionych strat.
5. DOKUMENTY WZORCOWE / FORMULARZE I ICH UŻYKOWNICY	III.E.4-F1 – Oświadczenie Członka Personelu MGGP S.A. /wzór/ – *Dyrektor/Menadżer/Lider/Asstent Obszaru lub wskazany w danym Obszarze / Biurze Pracownik* III.E.4-F2 – Porozumienie w sprawie używania sprzętu niebędącego własnością MGGP S.A. /wzór/ – *Dyrektor/Menadżer/Lider/Asstent Obszaru lub wskazany w danym Obszarze / Biurze Pracownik / ASI* III.E.4-F3 – Ankieta Dostawcy z zakresu bezpieczeństwa informacji /wzór/ – *Dyrektor/Menadżer/Lider/Asystent Obszaru lub wskazany w danym Obszarze / Biurze Pracownik / ASI / Koordynator ds. ODO / Pełnomocnik ZSZ*
6. ZAŁĄCZNIKI	III.E.4-Z1 Zasady bezpieczeństwa informacji

Formularz III.E.4-F1 Oświadczenie Członka Personelu MGGP S.A. /wzór/

OŚWIADCZENIE CZŁONKA PERSONELU* MGGP S.A.

Imię, nazwisko **pieczątka**	
Nr umowy	

Oświadczam, że zapoznałem się z treścią Wyciągu z Księgi Zintegrowanego Systemu Zarządzania w MGGP S.A., obejmującego następujące procedury:

III.E.1 Polityka Ochrony Danych Osobowych
III.E.1-Z1 Zasady postępowania z informacjami w wersji papierowej
III.E.4 Regulamin Użytkownika systemów informatycznych
III.E.6 Bezpieczeństwo fizyczne
Klasyfikacja informacji w MGGP S.A.

i zobowiązuję się do przestrzegania opisanych w nich zasad.

miejscowość, data ***Czytelny podpis członka Personelu MGGP S.A.***

*zgodnie z definicją w Słowniku do dokumentacji SZBI Personel obejmuje wszystkie osoby, które wykonują prace na rzecz Organizacji. Uszczegółowienie: obejmuje pracowników (zatrudnionych na podstawie umowy o pracę) oraz osoby współpracujące na podstawie innych stosunków prawnych.

Formularz III.E.4-F2 Porozumienie w sprawie używania sprzętu niebędącego własnością MGGP S.A. /wzór/

Porozumienie

zawarte w dniu _____, w _____, pomiędzy:

MGGP S.A. z siedzibą w Tarnowie**,** ul. Kaczkowskiego 6, 33-100 Tarnów, wpisaną do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla Krakowa Śródmieścia, XII Wydział Gospodarczy KRS pod nr 0000042514, NIP: 734-24-80-395, BDO: 000067410, Regon: 490808053, kapitał zakładowy w wysokości 2 300 000 zł, opłacony w całości, reprezentowaną przez:

_____

zwaną dalej MGGP

a

_____

zwanym dalej Użytkownikiem

Zważywszy, że:

1. Strony w dniu _____ zawarły umowę nr _____, której przedmiotem jest _____ (dalej: Umowa podstawowa),
2. Strony ustaliły, że zachodzi potrzeba aby Użytkownik przy realizacji Umowy podstawowej korzystał z urządzenia prywatnego: _____ (*wskazać rodzaj urządzenia*),
3. Zapisy obowiązującej w MGGP *Księgi Zintegrowanego Systemu Zarządzania Jakościowego, Środowiskowego, BHP i Bezpieczeństwem Informacji w Spółce MGGP S.A.* tj. punktu 4.6.1. Procedury III.E.4 *Regulamin Użytkownika systemów informatycznych* dopuszczają korzystanie z urządzeń prywatnych wyłącznie za zgodą MGGP S.A.,

Strony zawierają niniejsze porozumienie.

§ 1

1. Użytkownik oświadcza, że będzie realizował Umowę podstawową z wykorzystaniem urządzenia prywatnego: _____ (*wskazać rodzaj urządzenia i informacje identyfikujące dane urządzenie)* (dalej Urządzenie).
2. Użytkownik oświadcza, że:
   a. nośnik danych na Urządzeniu jest zaszyfrowany,
   b. na Urządzeniu zainstalowany jest system operacyjny w wersji posiadającej aktywne wsparcie techniczne producenta,
   c. system operacyjny jest na bieżąco aktualizowany/włączona automatyczna aktualizacja systemu,
   d. dostęp do Urządzenia jest zabezpieczony (np. hasło, kod PIN, blokada na podstawie linii papilarnych),
   e. urządzenie ma zainstalowany program antywirusowy i włączone automatyczne aktualizacje bazy sygnatur wirusów,
   f. Urządzenie nie jest udostępniane osobom trzecim,
   g. będzie sporządzał kopie zapasowe plików związanych z realizacją Umowy podstawowej, znajdujących się na Urządzeniu,
   h. oprogramowanie zainstalowane na Urządzeniu pochodzi z legalnego źródła, Użytkownik jest uprawniony do korzystania z oprogramowania, korzystanie z oprogramowania przez Użytkownika nie narusza praw osób trzecich.
3. Użytkownik zapewni, aby powyższe oświadczenia pozostawały aktualne przez cały okres korzystania z Urządzenia na potrzeby realizacji Umowy podstawowej.
4. Użytkownik jest odpowiedzialny za stan techniczny Urządzenia oraz rozwiązywanie ewentualnych problemów technicznych/merytorycznych związanych z korzystaniem z Urządzenia.
5. Korzystanie z Urządzenia przez Użytkownika następuje w ramach wynagrodzenia określonego w Umowie podstawowej. Użytkownikowi nie przysługuje żadne dodatkowe wynagrodzenie z korzystania z Urządzenia na potrzeby realizacji Umowy podstawowej, ani zwrot kosztów związanych lub wynikających z korzystania z Urządzenia.
6. MGGP nie ponosi odpowiedzialności za ewentualne szkody poniesione przez Użytkownika w związku z korzystaniem z Urządzenia na potrzeby realizacji Umowy podstawowej.
7. Użytkownik ponosi odpowiedzialność na zasadach ogólnych za wszelkie szkody poniesione przez MGGP w związku z korzystaniem z Urządzenia na potrzeby realizacji Umowy podstawowej. Użytkownik ponosi także odpowiedzialność za konsekwencje utraty danych przechowywanych na Urządzeniu.

§ 2

1. MGGP oświadcza, że wyraża zgodę na korzystanie przez Użytkownika z Urządzenia na potrzeby realizacji Umowy podstawowej.
2. Zgoda zostaje wydana na okres realizacji Umowy podstawowej.
3. Zgoda może zostać cofnięta w każdym czasie, w szczególności w przypadku stwierdzenia niezgodności Urządzenia z § 1 ust. 2.
4. W przypadku cofnięcia zgody lub wygaśnięcia niniejszego porozumienia Użytkownik jest obowiązany niezwłocznie, lecz nie później niż w terminie 1 dnia roboczego, trwale usunąć z Urządzenia wszelkie dane związane z realizacją Umowy podstawowej.

§ 3

1. Niniejsze porozumienie zostaje zawarte na okres obowiązywania Umowy podstawowej, z zastrzeżeniem że cofnięcie zgody, o którym mowa w § 2 ust. 3 jest równoznaczne z wygaśnięciem niniejszego Porozumienia.
2. Wszelkie zmiany niniejszego porozumienia wymagają dla swej ważności formy pisemnej.
3. Wszelkie ewentualne spory wynikające lub związane z niniejszym Porozumieniem Strony poddają rozstrzygnięciu sądu powszechnego właściwego dla MGGP.
4. Niniejsze porozumienie sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

Formularz III.E.4-F3 Ankieta Dostawcy z zakresu bezpieczeństwa informacji

ANKIETA ZGODNOŚCI DOSTAWCY Z WYMAGANIAMI ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z 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 (RODO) oraz PROCEDURAMI MGGP S.A. W OBSZARZE BEZPIECZEŃSTWA INFORMACJI
Ankieta dotyczy danych osobowych i innych danych stanowiących wartość dla MGGP S.A., które będą powierzane Dostawcy w trakcie realizacji umowy
MGGP S.A. w ramach prowadzonej działalności gospodarczej korzysta z pomocy podmiotów zewnętrznych, którym powierza przetwarzanie danych osobowych oraz inne dane stanowiące wartość dla MGGP S.A. W związku z powyższym MGGP S.A. jest zobowiązana dopełnić obowiązku weryfikacji podmiotów, z którymi współpracuje w zakresie obowiązków związanych z przetwarzaniem danych osobowych. Zgodnie z art. 28 ust. 1 RODO MGGP S.A. może korzystać wyłącznie z usług podmiotów, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie danych osobowych spełniało wymogi RODO oraz chroniło prawa osób, których dane dotyczą. Dodatkowo zgodnie z wdrożonym w MGGP S.A. Systemem Zarządzania Bezpieczeństwem Informacji na podstawie wymogów normy PN-ISO/IEC 27001, bezpieczeństwo informacji oraz systemów, w których są one przetwarzane jest jednym z kluczowych elementów polityki MGGP S.A. Dlatego dane stanowiące wartość dla MGGP S.A., Spółka może powierzyć wyłącznie temu podmiotowi, który gwarantuje sprawną i skuteczną ochronę danych przez zapewnienie odpowiedniego poziomu bezpieczeństwa oraz zastosowanie właściwych rozwiązań technicznych.

Nazwa Dostawcy	
Adres Dostawcy	
Dane kontaktowe Dostawcy	

Lp.	Pytanie	TAK / NIE / NIE DOTYCZY	Uwagi
1	Czy Dostawca posiada ważny certyfikat PN-EN ISO/IEC 27001 lub certyfikaty inne równoważne? Jeśli tak, należy wskazać jakie.		
2	Czy osoby przetwarzające dane osobowe w imieniu i na polecenie Dostawcy otrzymały upoważnienia do przetwarzania tych danych, z wyszczególnieniem zakresu przetwarzania (art. 29 RODO)?		
3	Czy Dostawca opracował i wdrożył politykę ochrony danych osobowych lub podobną procedurę (art. 24 RODO)?		
4	Czy osoby przetwarzające dane w imieniu i na polecenie Dostawcy zobowiązały się do zachowania w poufności tych danych oraz sposobów ich przetwarzania w trakcie i po zatrudnieniu (art. 29 RODO)?		
5	Czy osoby przetwarzające dane w imieniu i na polecenie Dostawcy zostały przeszkolone i zapoznane z przepisami o ochronie danych?		
6	Czy Dostawca prowadzi rejestr kategorii czynności przetwarzania (art. 30 RODO)?		
7	Czy Dostawca korzysta z usług tylko takich podmiotów zewnętrznych/podwykonawców, którzy gwarantują odpowiednie bezpieczeństwo danych osobowych (zgodność z RODO) oraz czy te podmioty zostały przez niego zweryfikowane?		
8	Czy Dostawca podpisał stosowne umowy powierzenia z podmiotami, którym przekazał do przetwarzania dane osobowe?		
9	Czy Dostawca korzysta z usług podmiotu, mającego siedzibę w państwie trzecim, o którym mowa w Rozdziale V RODO?		

10*	Czy Dostawca stosuje Standardowe klauzule umowne (lub inne środki, o których mowa w Rozdziale V RODO) wobec podwykonawców świadczących usługi poza obszarem Unii Europejskiej?		
11	Czy Dostawca stosuje środki kontroli dostępu fizycznego do budynku/budynków/obszarów przetwarzania danych osobowych?		
12	Czy dostęp do pomieszczeń pozostających w dyspozycji Dostawcy po godzinach pracy jest uniemożliwiony dla osób trzecich (np. firmy sprzątającej, firmy świadczącej usługi ochrony)?		
13*	W przypadku, gdy dostęp, o którym mowa pkt 12 jest możliwy, to czy jest on nadzorowany?		
14	Czy Dostawca wprowadził procedury wewnętrzne i środki bezpieczeństwa zapewniające zachowanie w tajemnicy innych danych, które jako informacje poufne, będą przekazywane Dostawcy w ramach współpracy z MGGP S.A.?		
15	Czy osoby przetwarzające inne dane w imieniu i na polecenie Dostawcy zobowiązały się do zachowania w poufności tych danych oraz sposobów ich przetwarzania w trakcie i po zatrudnieniu?		
16	Czy każdy użytkownik systemu informatycznego służącego do przetwarzania danych osobowych powierzanych przez Dostawcę otrzymuje indywidualny identyfikator?		
17	Czy Dostawca posiada formalne zasady zarządzania hasłami (minimalna długość, złożoność, częstotliwość zmiany, możliwość powtórnego użycia hasła, szyfrowanie przechowywanych haseł), które są wdrożone?		
18	Czy urządzenia np. tablety, smartfony i komputery, na których przetwarzane są dane osobowe, mają włączone automatyczne blokowanie ekranu po okresie bezczynności użytkownika?		
19	Czy Dostawca stosuje politykę tzw. „czystego biurka”?		
20	Czy dane osobowe i inne dane gromadzone w formie papierowej przechowywane są w zamykanych szafach/szufladach bez możliwości dostępu do nich osób nieupoważnionych?		
21	Czy Dostawca zabezpieczył kryptograficznie urządzenia przenośne oraz nośniki pamięci, wynoszone poza obszar przetwarzania?		
22	Czy Dostawca wdrożył politykę kopii zapasowych w odniesieniu do danych osobowych przetwarzanych w systemach informatycznych?		
23	Czy Dostawca zapewnił oprogramowanie antywirusowe na sprzęcie informatycznym (np. na komputerach stacjonarnych i przenośnych, telefonach komórkowych)?		

Ocena Dostawcy
WYPEŁNIA MGGP S.A.
[ ] Dostawca zapewnia/ odpowiednie środki technicznie i organizacyjne, w celu zapewnienia wymogów Rozporządzenia o Ochronie Danych Osobowych (RODO) oraz spełnia wymagania MGGP S.A. w obszarze bezpieczeństwa informacji.
[ ] Dostawca nie spełnia wymogów. Należy wybrać inny podmiot przetwarzający.

Załącznik III.E.4-Z1 Zasady bezpieczeństwa informacji

1. Dostawca zobowiązuje się przetwarzać powierzone mu do przetwarzania informacje wyłącznie w celu i zakresie wynikającym z niniejszej Umowy;
2. Dostawca gwarantuje pełną ochronę informacji przekazanych przez MGGP S.A. oraz ciągłość procesu ich przetwarzania;
3. Dostawca zapewnienia integralność i rozliczalność przetwarzanych informacji poprzez kontrolę nieautoryzowanego odczytywania, kopiowania, zmiany, usuwania lub przesyłu informacji oraz ochronę przed przypadkowym lub niezgodnym z prawem zniszczeniem lub utratą informacji.
4. Dostawca zapewni poprawne i bezpieczne funkcjonowanie wszystkich systemów przetwarzania informacji;
5. Dostawca maksymalnie ograniczy występowanie zagrożeń dla bezpieczeństwa informacji, które wynikają z celowej bądź przypadkowej działalności człowieka oraz ich ewentualne wykorzystanie na szkodę MGGP S.A.;
6. Dostawca zobowiązuje się nadać upoważnienia do przetwarzania informacji, z zastrzeżeniem osób, które podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy. Podwykonawca zapewnia, że osoby upoważnione do przetwarzania informacji zobowiążą się do zachowania tajemnicy lub że będą podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
7. Dostawca gwarantuje, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów tylko wtedy, gdy istnieje taka potrzeba;
8. Dostawca gwarantuje, że każdy pracownik upoważniony do przetwarzania informacji przeszedł szkolenie z zasad ochrony informacji, spełnia kryteria dopuszczenia do informacji i podpisał stosowne oświadczenie o zachowaniu poufności;
9. Dostawca zobowiązuje się do stałego nadzoru nad bezpieczeństwem przetwarzania informacji;
10. Dostawca zapewni gotowość do podjęcia działań w sytuacjach kryzysowych dla bezpieczeństwa MGGP S.A., jej interesów oraz posiadanych i powierzonych przez MGGP S.A. informacji;
11. Dostawca jest zobowiązany powiadomić w formie elektronicznej na adres mggp@mggp.com.pl niezwłocznie, jednak nie później niż w ciągu 24 godzin od powzięcia informacji, o wystąpieniu zdarzenia dotyczącego przetwarzania informacji MGGP, które może stanowić naruszenie bezpieczeństwa informacji.

Procedura III.E.6 Bezpieczeństwo fizyczne

Właściciel procesu: Obszar Wsparcia			
Wersja: 03	Kategoria jawności: II (wewnętrzne)	Obowiązuje od: 01.02.2024 r.	Stron: 2

1. CEL I PRZEDMIOT PROCEDURY	Celem dokumentu jest określenie zasad dotyczących bezpieczeństwa fizycznego i ochrony przed zagrożeniami środowiskowymi.
2. UCZESTNICY I ROLE W PROCEDURZE	**a) Zarząd:** - zapewnia niezbędne zabezpieczenia techniczne chroniące pomieszczenia organizacji; **b) Asystent Obszaru lub wskazany w danym Obszarze / Biurze Pracownik:** - prowadzi rejestr posiadaczy kluczy i kart dostępu w danym Obszarze; **c) Personel:** - odpowiada za przypisaną kartę dostępu, (i/lub) klucze, (i/lub) hasła do systemów alarmowych, a w przypadku zagubienia: *- karty / klucza / hasła niezwłocznie informuje o tym fakcie Koordynatora ds. ODO, Pracownika Działu IT/ASI, Pełnomocnika ZSZ oraz przełożonego i Asystenta Obszaru,* *- karta / hasła niezwłocznie informuje o tym fakcie Koordynatora ds. ODO, Pracownika Działu IT/ASI, Pełnomocnika ZSZ oraz przełożonego i Asystenta Obszaru,* - jest odpowiedziany za przebywanie osób z zewnątrz, z którymi umówił się na spotkanie, wykonanie pracy itp. w strefach MGGP, a w przypadkach opisanych w niniejszej procedurze musi uzyskać na to zgodę Zarządu lub/i zapewnić umowę poufności; **d) Obszar Wsparcia:** - dokonuje lub zapewnia przeprowadzenie okresowych przeglądów infrastruktury należącej do organizacji, - nadzoruje bezpieczeństwo fizyczne okablowania, - prowadzi zbiorczy rejestr kart dostępu, kluczy i haseł.
3. TERMINOLOGIA	Definicje stosowane w niniejszym dokumencie zawarte są w słowniku.
4. INSTRUKCJE POSTĘPOWANIA	
Nr 4.1	**Fizyczna granica obszaru bezpiecznego** 1.1.1. Na terenie należącym do organizacji zostały wydzielone obszary i strefy bezpieczeństwa. Dokładne opisy obszarów i zasady dostępu znajdują się w Formularzu III.E.6-F1 Opis stref i zasad dostępu.
Nr 4.2	**Nadzorowanie kluczy i kart dostępu** 4.2.1. Drzwi wejściowe do stref są otwierane za pomocą kart dostępu lub kluczy. 4.2.2. Karty dostępu oraz klucze są przekazywane do użytku tylko upoważnionym pracownikom przez pracowników odpowiedzialnych za zarządzanie kartami i kluczami w poszczególnych Obszarach. Każda karta dostępu jest przypisana do konkretnej osoby w systemie informatycznym. 4.2.3. Personel nie może udostępniać karty i kluczy innym osobom. 4.2.4. W przypadku zagubienia karty dostępu lub klucza ich użytkownik ma obowiązek zgłosić to Koordynatorowi ODO, który rejestruje ten fakt jako incydent. 4.2.5. W przypadku zagubienia karty dostępu, ASI dokonuje dezaktywacji karty w systemie kontroli dostępu. 4.2.6. W przypadku zagubienia klucza delegowany pracownik nadzoruje działania prowadzące do wymiany zamka.
Nr 4.3	**Zasady dostępu do poszczególnych obszarów** 4.3.1. Procedura zmiany haseł do systemu alarmowego. a) Hasła do systemu alarmowego są ustalane z agencją ochrony, która na mocy umowy z MGGP S.A. świadczy usługi w zakresie ochrony fizycznej i przekazywane w bezpieczny sposób osobom upoważnionym przez Zarząd. b) Zmiana haseł następuje w przypadku podejrzenia, że dotychczasowe hasło mogło być poznane przez nieuprawnione osoby. c) Użytkownik nie może udostępniać hasła innym osobom. d) W przypadku jakichkolwiek podejrzeń, że hasło poznała inna osoba, Użytkownik ma obowiązek zgłosić to ASI, który rejestruje ten fakt jako incydent. Dodatkowo należy zmienić hasło na nowe. e) W poszczególnych lokalizacjach MGGP, gdzie funkcjonują systemy alarmowe dedykowany pracownik prowadzi ewidencję dostępu do kodów alarmowych. 4.3.2. Zasady dostępu do obszarów poza godzinami pracy zostały opisane w *Formularzu III.E.6-F1 Opis stref i zasad dostępu*.
Nr 4.4	**Postępowanie z osobami z zewnątrz** 4.4.1 Członek personelu, który umówił się na spotkanie z osobami z zewnątrz ponosi odpowiedzialność za ich przebywanie w strefach. 4.4.2 Niedopuszczalne jest przebywanie osób z zewnątrz w jakiejkolwiek strefie bezpieczeństwa bez nadzoru personelu lub bez wcześniejszego podpisania klauzuli poufności. Przebywanie tego typu powinno być zgłoszone jako incydent. 4.4.3 Przebywanie i praca w strefach ekip remontowych, konserwacyjnych, sprzątających itp. może mieć miejsce wyłącznie za zgodą osób upoważnionych przez Zarząd. 4.4.4 W przypadku wykonywania prac przez podwykonawców (sprawy księgowo-kadrowe, usługi prawne, usługi techniczne itp.) z wykorzystaniem dokumentacji na poziomie dokumentów wewnętrznych lub poufnych, umowy zawarte z podwykonawcami muszą zawierać zapisy o poufności.

Nr 4.5	**Obszary publicznie dostępne, obszary dostaw i załadunku** 4.5.1. Obszar dostaw i załadunku znajduje się w sekretariatach / recepcjach (poszczególnych oddziałów) lub w sekretariacie znajdującym się w siedzibie organizacji. Można tam dokonywać nadania lub odbioru dostaw (np. poczty, paczek, cateringu) bez konieczności przyznawania dostępu nieupoważnionym osobom do obszarów bezpiecznych.
Nr 4.6	**Polityka dotycząca urządzeń i zabezpieczeń wspomagających bezpieczeństwo fizyczne** 4.6.1. Wszelkie zabezpieczenia techniczne chroniące pomieszczenia organizacji (system ppoż., alarmy, system monitoringu wizyjnego) są zapewnianie i nadzorowane przez organizację lub właściciela budynku na podstawie odpowiednich umów. 4.6.2. Wszystkie urządzenia wspomagające ochronę powinny spełniać wymagania obowiązujących przepisów. 4.6.3. Aby zagwarantować, że spełniono ww. przepisy należy zapewniać wyłącznie urządzenia posiadające odpowiednie atesty, certyfikaty lub aprobaty. 4.6.4. Należy zapewnić ciągłość bezpieczeństwa fizycznego poprzez redundancję (nadmiarowość) urządzeń i zabezpieczeń. Zaleca się utrzymywać jako minimum: a) zapasowe klimatyzatory w serwerowniach (lub klimatyzatory przenośne), b) zapasowe urządzenia UPS, c) zapasowe klucze do pomieszczeń, szafek i sejfów, d) zapasowe karty dostępu, e) dodatkowe gaśnice, f) zapasowy dostęp do internetu.
Nr 4.7	**Polityka dotycząca lokalizacji i bezpieczeństwa fizycznego sprzętu** 4.7.1. Urządzenia przetwarzające Dane powinny zostać umieszczone w taki sposób, by zminimalizować niepożądany dostęp do obszarów roboczych w ramach stref bezpieczeństwa oraz ograniczyć do minimum brak nadzoru podczas ich użytkowania. 4.7.2. Najważniejsze urządzenia powinny zostać rozmieszczone w strefach bezpiecznych tak, aby wykluczyć publiczny dostęp do nich. Dotyczy to przede wszystkim serwerów, komputerów lokalnych i przenośnych oraz drukarek sieciowych, kserokopiarek i urządzeń faksowych. 4.7.3. Przetwarzanie informacji (np. wydruk, kserokopia) za pomocą urządzeń znajdujących się w strefie publicznej musi być pod nadzorem osób upoważnionych do przetwarzania. Obowiązuje ścisły zakaz pozostawiania bez opieki dokumentów i nośników zawierających informacje inne niż publiczne w strefach.
Nr 4.8	**Polityka dotycząca bezpieczeństwa fizycznego okablowania** 4.8.1. Okablowanie telekomunikacyjne powinno być chronione przed podsłuchem lub uszkodzeniem. Jeśli tylko jest to technicznie możliwe, to należy unikać wyznaczania tras kabli biegnących przez obszary publiczne. 4.8.2. Wszystkie punkty rozdzielcze sieci powinny (w miarę możliwości technicznych) znajdować się w zamykanych skrzynkach lub szafach teleinformatycznych umieszczonych w zamykanych pomieszczeniach. 4.8.3. Należy oddzielać kable zasilające od okablowania komunikacyjnego w celu uniknięcia interferencji. Jeśli nie jest to możliwe należy używać okablowania ekranowanego. 4.8.4. Należy stworzyć system jednoznacznego oznakowania umożliwiającego identyfikację kabli i sprzętu w celu zmniejszenia ryzyka błędów nieumyślnego połączenia kabla sieciowego. 4.8.5. Szczegółowe wymagania odnośnie konfiguracji i zabezpieczenia sieci zostały opisane w Procedurze *III.E.2 Instrukcja zarządzania systemem informatycznym*. 4.8.6. Za nadzór nad bezpieczeństwem fizycznym okablowania odpowiada Dział IT.
Nr 4.9	**Przeglądy infrastruktury dla bezpieczeństwa fizycznego** 4.9.1. W celu zapewnienia właściwego bezpieczeństwa fizycznego Obszar Wsparcia powinien dokonywać okresowych przeglądów infrastruktury należącej do organizacji zgodnie z ustalonym Harmonogramem przeglądów. 4.9.2. Harmonogram powinien uwzględniać wymagania prawa budowalnego, zalecenia producentów urządzeń oraz wyniki szacowania ryzyka. 4.9.3. Jako minimum należy dokonywać: a) przeglądów instalacji ppoż. b) przeglądów instalacji alarmowej, c) przeglądów instalacji elektrycznej, d) przeglądów urządzeń klimatyzacyjnych, e) sprawdzenia skuteczności zamków w drzwiach do poszczególnych stref, f) sprawdzenia skuteczności działania systemu dostępowego, g) sprawdzenia działania systemu monitoringu wizyjnego, h) przegląd aktualności uprawnień kart dostępowych i kluczy, i) przegląd osób mających dostęp do kodów systemów alarmowych.
5. DOKUMENTY WZORCOWE / FORMULARZE I ICH UŻYKOWNICY	III.E.6-F1 – Opis stref i zasad dostępu – *ASI*
6. ZAŁĄCZNIKI	III.E.6-Z1 – Zasady postępowania z kluczami i kartami dostępu do budynków/pomieszczeń MGGP S.A.

Załącznik III.E.6-Z1 Zasady postępowania z kluczami i kartami dostępu do budynków/pomieszczeń MGGP S.A.

MGGP GRUPA MGGP	**Zasady postępowania z kluczami i kartami dostępu do budynków i pomieszczeń MGGP S.A.**		
Wersja: 01	Kategoria jawności: II (wewnętrzne)	Obowiązuje od: 01.02.2024 r.	Stron: 2

Cele wprowadzenia zasad postępowania z wszystkimi środkami kontroli dostępu do pomieszczeń:

1. Niniejszy dokument stanowiący instrukcję postępowania z kluczami i kartami dostępu do budynków i pomieszczeń w MGGP S.A. ma za zadanie zredukować ryzyko niespodziewanego wejścia w obszar przetwarzania osoby nieupoważnionej oraz umożliwić poufne składowanie dokumentacji MGGP S.A. (**Administrator**);
2. Stosowanie zasad oraz wdrożenie procedur określonych w niniejszej Instrukcji ma na celu zapewnienie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających dane osobowe oraz utrzymania bezpieczeństwa ich przetwarzania;
3. Niniejsza Instrukcja została opracowana w oparciu o powszechnie obowiązujące przepisy prawa z zakresu ochrony danych osobowych i jej treść odpowiada wymaganiom stawianym w szczególności przez 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 (Dz. Urz.UE.L Nr 119, str. 1), zwanego dalej **RODO**;
4. RODO nakazuje, aby dane osobowe były dostępne wyłącznie dla osób upoważnionych (zarówno w strukturze Administratora, jak i po stronie podmiotów powiązanych - np. właściciela budynku) oraz aby samo przetwarzanie odbywało się na polecenie Administratora. Zarządzanie kluczami służy kontroli dostępu do danych składowanych i przetwarzanych w biurze Administratora, w postaci papierowej oraz pośrednio, w postaci cyfrowej;
5. Instrukcja ma również redukować ryzyko kradzieży majątku Administratora, w tym narzędzi pracy takich jak m.in. komputerów i nośników, w pamięci których mogą być przechowywane dane osobowe;

Niniejsza Instrukcja obowiązuje wszystkie osoby z personelu Administratora, niezależnie od podstawy prawnej współpracy.

Rozdział I
Postanowienia ogólne

§ 1

1. Użyte w niniejszej Instrukcji określenia oznaczają:
   a) **Pomieszczenia MGGP** – pomieszczenia, w których MGGP S.A. wykonuje swoją działalność, zlokalizowane w budynkach będących własnością MGGP S.A. lub przez nią wynajmowanych,
   b) **Personel** – wszystkie osoby, które wykonują prace na rzecz Organizacji; obejmuje pracowników (zatrudnionych na podstawie umowy o pracę) oraz osoby współpracujące na podstawie innych stosunków prawnych.
2. Szczegółowe zasady dotyczące bezpieczeństwa fizycznego określa procedura III.E.6 Bezpieczeństwo fizyczne Księgi Zintegrowanego Systemu Zarządzania jakościowego, środowiskowego, BHP i bezpieczeństwem informacji w Spółce MGGP S.A.

Rozdział II
Stosowane środki kontroli dostępu i odpowiedzialność za nie

§ 2

1. Budynki, w których zlokalizowane są pomieszczenia biurowe Administratora znajdują się na terenach wydzielonych i/lub ogrodzonych z wyznaczonymi zamykanymi bramami wjazdowymi oraz nadzorowanymi przez personel Administratora. Budynki podlegają ochronie polegającej na całodobowym monitorowaniu przez system alarmowy.
2. W lokalizacjach posiadających systemy alarmowe prowadzona jest ewidencja osób posiadających kod dostępu do systemu alarmowego i klucz do szyfratora.
3. Pomieszczenia biurowe indywidualne, jak również pomieszczenia przeznaczone do prowadzenia spotkań, wydzielone są drzwiami w standardzie biurowym, wyposażonymi w zamki lub znajdują się na zamykanym piętrze/poziomie.
4. Dokumenty zawierające dane osobowe, nośniki zawierające dane osobowe oraz komputery przenośne stosowane przez Personel Administratora przechowywane są w meblach zamykanych na klucz w pomieszczeniach zabezpieczonych fizycznie przed dostępem osób nieupoważnionych.
5. Niniejsza Instrukcja służy, w pierwszej kolejności, ustaleniu standardu postępowania z kluczami do tych właśnie środków kontroli dostępu.

Rozdział III
Zabezpieczenie pomieszczeń i procedura postępowania z kluczami oraz kartami dostępu do pomieszczeń MGGP S.A.

§ 3

1. Zasady dotyczące obowiązku przechowywania dokumentów w sposób poufny określają procedury Księgi Zintegrowanego Systemu Zarządzania jakościowego, środowiskowego, BHP i bezpieczeństwem informacji w Spółce MGGP S.A.
2. Dokumenty papierowe lub nośniki zawierające dane osobowe lub dane mające wartość dla Organizacji, które zgodnie z zakresem realizowanych obowiązków, przetwarzane są wyłącznie przez określonych Członków Personelu, składowane są w szafach zamykanych na klucz, do których dostęp posiadają wyłącznie te osoby. Członkowie Personelu, którym zostały powierzone klucze i/lub karty dostępu zobowiązani są do:
   a) wykorzystywania ich zgodnie z przeznaczeniem,
   b) niekopiowania powierzonych kluczy bez zgody Dyrektora Obszaru oraz nieudostępniania ich osobom trzecim,
   c) nieudostępniania powierzonych kart dostępu osobom trzecim,
   d) zamykania na klucz pomieszczeń biurowych, w których chwilowo nie przebywa dany Członek Personelu,
   e) po otwarciu pomieszczenia biurowego, przed przystąpieniem do pracy do sprawdzenia stanu zastosowanych zabezpieczeń sprzętu biurowego, komputerowego, a także składowanej w tym pomieszczeniu dokumentacji i innego wyposażenia,
   f) w przypadku stwierdzenia zmian lub naruszenia stanu zabezpieczeń, Członek Personelu, który to stwierdził, natychmiast powiadamia o tym swojego bezpośredniego i kierownika jednostki,

g) po zakończeniu pracy, uporządkowania swoich stanowisk pracy, wykonania czynności zabezpieczających adekwatnych do stosownych rozwiązań technicznych i organizacyjnych, w szczególności: zabezpieczenia komputerów i wszelkich nośników danych, wyłączenia wszystkich urządzeń elektrycznych (nie wymagających zasilania), zamknięcia wszystkich okien i drzwi,
h) zgłoszenia właściwym osobom zagubienia klucza/kluczy lub karty dostępu:
   - w przypadku zagubienia karty dostępu lub klucza ich użytkownik ma obowiązek zgłosić do Koordynatora ODO, który rejestruje ten fakt jako incydent,
   - w przypadku zgubienia karty dostępu, pracownik ASI dokonuje dezaktywacji karty w systemie kontroli dostępu,
   - w przypadku zagubienia klucza delegowany pracownik nadzoruje działania prowadzące do wymiany zamka.

3. Klucze od biurek i szaf biurowych są w posiadaniu Członków Personelu, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.
4. Wzory oświadczeń Członka Personelu o przyjęciu klucza/karty dostępu stanowią załączniki do niniejszej Instrukcji.
5. Dyrektor Obszaru w danej lokalizacji wyznacza osobę odpowiedzialną za należyte przechowywanie, zabezpieczenie oraz udostępnianie kluczy zapasowych, które przechowywane są w zamkniętej skrzynce/gablocie bez dostępu dla pozostałych Członków Personelu.
6. Wydawanie kluczy zapasowych (o których mowa w ust. 7) Członkom Personelu może odbywać się tylko w uzasadnionych sytuacjach oraz w przypadkach awaryjnych.
7. Klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić do osoby wydającej.

Z uwagi na odrębne specyfikacje lokalowe poszczególnych lokalizacji MGGP S.A., każda z nich posiada odrębnie ustalone zasady zamykania pomieszczeń w nich zlokalizowanych. Jednakże każda z nich prowadzi ewidencję posiadaczy kluczy i kart dostępu.

DOKUMENTY WZORCOWE / FORMULARZE I ICH UŻYKOWNICY	III.E.6-Z1-F2 – Ewidencja kart dostępu – *Asystent Obszaru lub wskazany w danym Obszarze / Biurze Pracownik, ewidencja zbiorcza – Obszar Wsparcia* III.E.6-Z1-F3 – Rejestr posiadaczy kluczy – *Asystent Obszaru lub wskazany w danym Obszarze / Biurze Pracownik, ewidencja zbiorcza – Obszar Wsparcia* III.E.6-Z1-F4 – Wzór Oświadczenia Członka Personelu MGGP S.A. o przyjęciu karty dostępu – *Asystent Obszaru lub wskazany w danym Obszarze / Biurze Pracownik* III.E.6-Z1-F5 – Wzór Oświadczenia Członka Personelu MGGP S.A. o przyjęciu kluczy do pomieszczeń MGGP S.A. – *Asystent Obszaru lub wskazany w danym Obszarze / Biurze Pracownik* III.E.6-Z1-F6 – Wykaz osób posiadających dostęp do kluczy zapasowych w lokalizacji (wzór) – *Asystent Obszaru lub wskazany w danym Obszarze / Biurze Pracownik* III.E.6-Z1-F7 – Oświadczenia członka personelu MGGP S.A. o przyjęciu kodu dostępu wraz z kluczem do szyfratora (wzór) – *Pracownik Działu IT lub wskazany w danym Obszarze / Biurze Pracownik*

Klasyfikacja informacji w MGGP S.A.

Zgodnie z procedurą III.E.5 Zarządzanie Systemem Zarządzania Bezpieczeństwem Informacji w MGGP S.A. ustalono podział informacji na 3 kategorie:

a) **Informacje chronione (I)**
b) **Informacje wewnętrzne (II)**
c) **Informacje publiczne (III)**

Lp.	Kategoria jawności	Charakterystyka informacji	Dostęp	Postępowanie z informacją	Przykłady dokumentów*
1.	**Chronione**	Do grupy informacji chronionej zakwalifikowane zostały między innym dane typu: • Dane Osobowe • wymagania umowne • dane kontaktowe kontrahentów • niepubliczne dane finansowe Firmy • niepubliczne dane finansowe kontrahentów • dokumentacja zabezpieczeń fizycznych • zapisy zdarzeń z systemów monitorujących • logi systemowe z systemów przechowywania i przetwarzania informacji • informacje stanowiące tajemnicę przedsiębiorstwa MGGP S.A. Dostęp do grupy informacji chronionej jest przyznawany przez Zarząd lub osobę wyznaczoną. Czas dostępu jest z góry określony i wynika z pełnionej roli. Konkretne prawa dostępu realizowane są poprzez systemy, w których informacja jest przetwarzana. Prawa dostępu i uprawnienia są rozgraniczone i realizowane na podstawie ról pełnionych przez pracowników.	- dostępne tylko dla upoważnionych osób - dostępne dla stron zewnętrznych tylko na podstawie umowy - Dane Osobowe mogą być udostępnione tylko na podstawie Upoważnień lub Umów powierzenia	- dostęp do informacji jest określony dla ograniczonej liczby osób - można się dzielić informacją za pozwoleniem osoby upoważnionej przez Zarząd Organizacji - informacja/dane mogą być umieszczane tylko na serwerach z uwierzytelnionym dostępem - informacja nie może być kopiowana, powielana bez zgody Zarządu lub osób upoważnionych Każdy członek personelu będący w posiadaniu informacji chronionej jest zobowiązany do zachowania poufności informacji i nie ujawniania jej osobom nieupoważnionym. Dostęp do informacji osoba może utracić na skutek – zakończenia współpracy, zmiany zajmowanego stanowiska, naruszenia zasad bezpieczeństwa informacji. Przechowując i wykorzystując w pracy informacje chronione, należy zachować szczególne środki ostrożności, aby nie ujawnić jej innym członkom personelu oraz stronom zewnętrznym. Informacje chronione są przechowywane przy wykorzystaniu bezpiecznych systemów. Stosowana jest zwiększona kontrola przy dostępie do tego typu informacji.	• Dane kadrowe pracowników / współpracowników • Umowy o pracę / umowy zlecenia / umowy o dzieło i in. • Umowy z podwykonawcami / dostawcami usług • Umowy z klientami • Dokumenty związane z realizacją kontraktów (notatki, protokoły, faktury, korespondencja i in.) • Umowy z dostawcami usług okołoprodukcyjnych • Dokumentacja organów Spółki (np. uchwały i protokoły Zarządu / Rady Nadzorczej/ Walnego Zgromadzenia Spółki • Dokumenty finansowe Spółki (np. umowy kredytowe) • Polisy i gwarancje • Oferty handlowe i przetargowe
2.	**Wewnętrzne**	Do grupy informacji wewnętrznych zostały zakwalifikowane dane typu:	- dostępne dla całego personelu Organizacji	- można dzielić się tą informacją z innymi członkami personelu firmy	• Biuletyn MGGP S.A. • Regulamin Pracy i inne regulaminy MGGP S.A. • Księga Zintegrowanego Systemu Zarządzania

		• ogólne instrukcje, procedury, wymagania • regulaminy • umiejscowienie pomieszczeń strategicznych (Zarządu, kadr i finansów, serwerowni).	- dostępne dla stron zewnętrznych tylko na podstawie umowy	- informacja może być umieszczona na wewnętrznym serwerze - można posiadać kopie danych na lokalnej stacji roboczej - informacja może być pozostawiana na biurku	• Komunikaty Biura Zarządu • Przewodnik po MGGP S.A. • Wszelkie dokumenty udostępnione w systemie BINDER - ZASOBY
3.	**Publiczne**	Do grupy informacji publicznej zostały zakwalifikowane dane zlokalizowane w ogólnie dostępnych miejscach, np. na stronach www, w ogłoszeniach prasowych, rejestrach (np. Regon, KRS, CEIDG) itd. oraz dane ujawniane szerokiemu kręgowi adresatów. Są to np. dane kontaktowe (w tym firmowe dane kontaktowe członków personelu) ogólny zakres działalności, komunikaty.	- dostępne dla wszystkich stron	- można się dzielić informacją z osobami trzecimi	• Informacje ujawniane w ogólnodostępnych rejestrach i MSiG, np.: w KRS, CRBR • Informacje umieszczane w social mediach MGGP S.A. i na stronie internetowej Spółki • Imię, nazwisko, numer telefonu służbowego, stanowisko oraz adres mailowy członka personelu MGGP S.A.

*wymienione dokumenty nie są katalogiem zamkniętym

Pamiętaj!
W przypadku wątpliwości co do kategoryzacji dokumentu skonsultuj się z Przełożonym lub autorem dokumentu.