



Gramm Technika
Sp. z o.o.
Karolewo 5
66-300 Międzyrzecz

POLITYKA

WYDANIE: II/2023

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

WPROWADZONO
DNIA:

09.05.2018

OBOWIĄZUJE OD:

25.05.2018

**POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH
OSOBOWYCH – GRAMM TECHNIKA SP Z O.O.**

GRAMM TECHNIKA SP. Z O.O.


KAROLEWO 5

66-300 MIĘDZYRZECZ

Zatwierdzono:	Andrzej Kozuch
Podpis:	
Wydanie:	2 / 2023-10-03

SPIS TREŚCI

SPIS TREŚCI.....	2
1. Cel wprowadzenia polityki.....	3
1.1. Informacje ogólne.....	3
1.2. Zakres zastosowania Polityki Bezpieczeństwa.....	3
1.3. Terminy zastosowane w Polityce Bezpieczeństwa	5
2. Osoby odpowiedzialne za ochronę danych osobowych.....	7
2.1. Informacje ogólne.....	7
2.2. Administrator Danych.....	7
2.3. Administrator Systemów Informatycznych	9
2.4. Osoby upoważnione do przetwarzania danych osobowych.....	9
3. Indywidualne upoważnienie do przetwarzania danych osobowych	10
4. Umowy powierzenia przetwarzania danych osobowych.....	11
5. Ogólne zasady bezpieczeństwa obowiązujące przy przetwarzaniu danych osobowych.....	12
6. Instrukcja postępowania w sytuacji naruszenia zasad ochrony danych osobowych	14
7. Postanowienia końcowe.....	15
8. Załączniki	16

 Gramm Technika Sp. z o.o. Karolewo 5 66-300 Międzyrzecz	POLITYKA BEZPIECZEŃSTWA		WYDANIE: I/2018	
	INSTRUKCJA - OCENA RYZYKA PRZETWARZANIA DANYCH			
	WPROWADZONO DNIA:	9.05.2018	OBOWIĄZUJE OD:	25.05.2018

1. CEL WPROWADZENIA POLITYKI BEZPIECZEŃSTWA


1.1. INFORMACJE OGÓLNE

Celem Wprowadzenia Polityki Bezpieczeństwa w Gramm Technika Sp. z o.o. jest spełnienie wymagań ustawodawcy o obowiązku wynikającym z przepisów dotyczących ochrony danych osobowych oraz z Rozporządzenia Parlamentu Europejskiego i Rady dążących w swoim zamyśle przede wszystkim do ochrony prywatności i godności każdego pracownika oraz klientów i interesantów Organizacji Gramm Technika Sp. z o. o.

1. Wprowadzenie Polityki Bezpieczeństwa ma na celu zapewnienie zgodności działań Administratora Danych z Ustawą o ochronie danych osobowych oraz jej rozporządzeniami wykonawczymi, a także z Rozporządzeniem Parlamentu Europejskiego i Rady 2016/679.
2. Polityka Bezpieczeństwa została opracowana zgodnie z wytycznymi zawartymi w:
 - a) Ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 nr 133 poz. 883);
 - b) Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. 2004 nr 100 poz. 1024);
 - c) Rozporządzeniu Parlamentu Europejskiego i Rady 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchyleniu dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).


1.2. ZAKRES ZASTOSOWANIA POLITYKI BEZPIECZEŃSTWA

1. Polityka Bezpieczeństwa określa zasady i tryb postępowania przy uzyskiwaniu, wykorzystywaniu, przetwarzaniu danych osobowych, w tym danych przetwarzanych w systemie informatycznym i poza nim, a także zabezpieczenia danych przed nieuprawnionym dostępem.
2. Polityka Bezpieczeństwa dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny, tj. w formie papierowej jak i w systemach informatycznych.
3. Procedury i zasady określone w Polityce Bezpieczeństwa stosuje się do wszystkich osób, zarówno zatrudnionych na podstawie umowy o pracę, oraz umów cywilnoprawnych.
4. Zakresem zastosowania Polityki Bezpieczeństwa objęci są wszyscy pracownicy pracujący na rzecz Organizacji, których danymi osobowymi Organizacja dysponuje, rozporządza, przetwarza, wszyscy Interesanci Organizacji, których danymi Organizacja dysponuje, rozporządza, bądź przetwarza, Klienci indywidualni, nie będący Osobami Prawnymi, których danymi osobowymi organizacja

 Gramm Technika Sp. z o.o. Karolewo 5 66-300 Międzyrzecz	POLITYKA BEZPIECZEŃSTWA		WYDANIE: I/2018	
	INSTRUKCJA - OCENA RYZYKA PRZETWARZANIA DANYCH			
	WPROWADZONO DNIA:		OBOWIĄZUJE OD:	

dysponuje, rozporządza i przetwarza. W szczególności zaś Polityka Bezpieczeństwa dotyczy osób bezpośrednio zajmujących się przetwarzaniem i wykorzystywaniem danych osobowych wszystkich osób wcześniej wymienionych na rzecz Organizacji i jej działalności.


5. W związku z przetwarzaniem danych w systemach informatycznych opracowano „**Instrukcję zarządzania systemem informatycznym**” służącym do przetwarzania danych osobowych – jest to Załącznik nr 9 do Polityki Bezpieczeństwa i stanowi jej integralną część.

 Gramm Technika Sp. z o.o. Karolewo 5 66-300 Międzyrzecz	POLITYKA BEZPIECZEŃSTWA		WYDANIE: I/2018	
	INSTRUKCJA - OCENA RYZYKA PRZETWARZANIA DANYCH			
	WPROWADZONO DNIA:		OBOWIĄZUJE OD:	


1.3. TERMINY ZASTOSOWANE W POLITYCE BEZPIECZEŃSTWA

Podstawowe terminy użyte w Polityce bezpieczeństwa i ich znaczenia:

1. Ustawa – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. 2015 poz. 2135).
2. Rozporządzenie – rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).
3. Rozporządzenie RODO - Rozporządzenie Parlamentu Europejskiego i Rady 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchyleniu dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
4. Gramm – Organizacja Gramm Technika Sp. z o.o. z siedzibą w Karolewie 5.
5. Administrator Danych - administrator danych osobowych (ADO) – Gramm Technika Sp. z o.o., która decyduje o celach i środkach przetwarzania danych osobowych w firmie oraz monitoruje wdrożone zabezpieczenia systemu informatycznego.
6. Administrator systemu informatycznego (ASI) – osoba, organizacja odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych, w tym w szczególności za przeciwdziałanie dostępowi osób nieupoważnionych do systemów oraz podejmowanie odpowiednich działań w przypadku stwierdzenia naruszeń w tych systemach.
7. Ewidencja osób upoważnionych do przetwarzania danych osobowych – wykaz osób upoważnionych i zobowiązanych pokazujący m.in. do czego są upoważnieni poszczególni pracownicy.
8. Hasło – ciąg znaków literowych, cyfrowych lub innych, znanych jedynie osobie upoważnionej do pracy w systemie informatycznym.
9. Osoba upoważniona – osoba, która została pisemnie upoważniona przez administratora danych do przetwarzania danych osobowych.
10. Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, w szczególności wszystkie dane które mogą mieć wpływ na życie prywatne i rodzinne, prawo do komunikowania się, wolności myśli, sumienia, religii, wolności wypowiedzi i informacji, prawo do różnorodności kulturowej, religijnej i językowej, a także wszelkie informacje dotyczące stanu zdrowia osoby, której dane dotyczą.
11. Umowa powierzenia danych osobowych – umowa z organizacją zewnętrzną, która świadczy na rzecz Gramm określone usługi, w zakresie których znajdują się operacje dotyczące dysponowania, przetwarzania i posiadania danych osobowych pracowników i interesantów Gramm.

 Gramm Technika Sp. z o.o. Karolewo 5 66-300 Międzyrzecz	POLITYKA BEZPIECZEŃSTWA		WYDANIE: I/2018	
	INSTRUKCJA - OCENA RYZYKA PRZETWARZANIA DANYCH			
	WPROWADZONO DNIA:		OBOWIĄZUJE OD:	

12. Osoba możliwa do zidentyfikowania – każda osoba fizyczna, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności poprzez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.
13. Zbiór danych osobowych – posiadający strukturę zestaw danych o charakterze danych osobowych, które są dostępne według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
14. Przetwarzanie danych osobowych – jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
15. System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych; za system informatyczny uważany jest również pojedynczy komputer wraz z oprogramowaniem, przy pomocy którego przetwarzane są dane osobowe.
16. Ocena ryzyka dla wolności i praw osób, których dane dotyczą – ocena wykonana przez Gramm na podstawie ustalonego sposobu postępowania mająca na celu określenie czy występuje ryzyko naruszenia praw, lub wolności osób fizycznych.
17. Zabezpieczenie danych w systemie informatycznym – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
18. Ocena skutków dla ochrony danych osobowych – należy ją przeprowadzić, gdy ocena ryzyka wykaże, że planowane działania z dużym prawdopodobieństwem mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.
19. Usuwanie danych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
20. Zgoda osoby, której dane dotyczą – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie; zgoda może dotyczyć tylko określonego rodzaju przetwarzania danych, każdy inny rodzaj przetwarzania danych wymaga uzyskania zgody – na każdy kolejny sposób przetwarzania.
21. Rejestr naruszeń ochrony danych osobowych – rejestr sporządzony do dokumentowania ewentualnych naruszeń ochrony danych osobowych.
22. Instrukcja – Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Gramm Technika Sp. z o.o.

 Gramm Technika Sp. z o.o. Karolewo 5 66-300 Międzyrzecz	POLITYKA BEZPIECZEŃSTWA		WYDANIE: I/2018	
	INSTRUKCJA - OCENA RYZYKA PRZETWARZANIA DANYCH			
	WPROWADZONO DNIA:		OBOWIĄZUJE OD:	


2. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

2.1. INFORMACJE OGÓLNE

- Osoby odpowiedzialne za dostęp i przetwarzanie danych w Organizacji Gramm, są zobowiązane do przetwarzania danych osobowych oraz ich ochronę zgodnie z postanowieniami Ustawy, Rozporządzenia, Rozporządzenia RODO i Polityki Bezpieczeństwa oraz Instrukcji zarządzania system informatycznym.
- Osobami odpowiedzialnymi za przetwarzanie danych osobowych w Gramm Technika są:
 - Administrator Danych.
 - Administrator Systemów Informatycznych.
 - Osoby upoważnione, w tym osoby i instytucje upoważnione na mocy umowy z Gramm o dostępie, administrowaniu i zarządzaniu danymi osobowymi na określone jasno sprecyzowane cele.
- Ww. osoby zobowiązane są przestrzegać zasad bezpieczeństwa danych określonych w polityce bezpieczeństwa, w przepisach prawa krajowego i międzynarodowego, w szczególności z postanowieniami Ustawy, Rozporządzenia, Rozporządzenia RODO i Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemami informatycznymi, a także współpracować we wdrażaniu oraz doskonaleniu procedur ochrony informacji. Zgłaszają uwagi i opiniują zastosowane rozwiązania.
- Osoby odpowiedzialne za przetwarzanie danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia także po ustaniu zatrudnienia.


2.2. ADMINISTRATOR DANYCH

- Administrator danych Gramm Technika Sp. z o.o., zwany dalej Gramm – reprezentowany przez V-ce Prezesa Zarządu.
- Administrator danych:
 - Jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
 - Administrator danych informuje o sposobie i celu przetwarzania danych (obowiązek informacyjny). Administrator danych musi zapewnić, że zgromadzone dane osobowe są poprawne i aktualne (możliwość wprowadzania korekt), a ich przetwarzanie przebiega bez zakłóceń.
 - Upoważnia poszczególne osoby do przetwarzania danych osobowych w indywidualnym zakresie, odpowiadającym zakresowi ich zadań i obowiązków, w oparciu o załącznik nr 6 – „**Arkusze identyfikacji przetwarzania danych osobowych, wykaz zbiorów danych**”

 Gramm Technika Sp. z o.o. Karolewo 5 66-300 Międzyrzecz	POLITYKA BEZPIECZEŃSTWA		WYDANIE: I/2018	
	INSTRUKCJA - OCENA RYZYKA PRZETWARZANIA DANYCH			
	WPROWADZONO DNIA:		OBOWIĄZUJE OD:	

przetwarzanych”, a także podpisuje umowy powierzenia przetwarzania danych osobowych, załącznik nr 3 - „**Umowa powierzenia przetwarzania danych osobowych**”.

- d) Inicjuje i bierze czynny udział w ocenie ryzyka dla wolności i praw osób, których dane dotyczą, jeżeli ocena tego wymaga inicjuje i bierze czynny udział w ocenie skutków dla ochrony danych osobowych.
 - e) W razie stwierdzenia lub podejrzenia naruszenia zasad przetwarzania i ochrony danych osobowych, w szczególności wypłynięcia tych danych mogących prowadzić do zidentyfikowania lub możliwości zidentyfikowania osoby fizycznej, danych które mogą mieć wpływ na życie prywatne i rodzinne, prawo do komunikowania się, wolności myśli, sumienia, religii, wolności wypowiedzi i informacji, prawo do różnorodności kulturowej, religijnej i językowej, a także wszelkie informacje dotyczące stanu zdrowia osoby, której dane dotyczą, a także zagrożenia zabezpieczeń systemu informatycznego, w tym na wniosek administratora bezpieczeństwa informacji - podejmuje odpowiednie działania w celu usunięcia zagrożenia lub minimalizacji jego skutków.
 - f) W przypadku stwierdzenia naruszenia ochrony danych osobowych, a w szczególności naruszenia danych osobowych skutkujących uszczerbkiem fizycznym, szkodą majątkową, lub niemajątkową osoby której dane dotyczą – Administrator ma obowiązek zgłosić takie naruszenie organowi nadzorcemu nie później niż 72 godziny – jeżeli jest to wykonalne.
 - g) Jeżeli dane osobowe zostały utracone – Administrator powinien bez zbędnej zwłoki powiadomić osobę, której dane zostały utracone – w przypadku gdy utrata tych danych może zagrozić prawom, lub wolnościom tej osoby.
 - h) Jeżeli dane osobowe zostały naruszone Administrator Danych ma obowiązek upewnić się, że „**Rejestr naruszeń ochrony danych osobowych**” – zał. nr 8 został zaktualizowany o dane naruszenie, oraz wszelkie czynności wymagane przez niniejszą Politykę Bezpieczeństwa zostały podjęte w celu zminimalizowania zagrożenia dla bezpieczeństwa osoby, której dane dotyczyły.
 - i) Administrator udostępnia dane osobowe ze zbioru, na żądanie uprawnionych podmiotów, w przypadkach wskazanych prawem.
 - j) Administrator Danych wydaje „**Indywidualne upoważnienia do przetwarzania danych osobowych**” – zał. nr 1 wszystkim osobom, które biorą udział w procesie przetwarzania danych osobowych.
 - k) Administrator Danych podpisuje umowy powierzenia z podmiotami zewnętrznymi, którym Gramm powierza, bądź zamierza powierzyć dane osobowe. Powierzenie przetwarzania danych, w imieniu i na rzecz Gramm odrębnemu podmiotowi może przebiegać tylko i wyłącznie z zachowaniem zasad przywołanych w niniejszej Polityce Bezpieczeństwa. Lista zewnętrznych podmiotów i organizacji, którym powierzono przetwarzanie danych osobowych na rzecz Gramm znajduje się w zał. nr 4 - „**Wykaz podmiotów, którym Administrator Danych powierzył przetwarzanie danych osobowych**”.
3. Administrator danych może powołać administratora bezpieczeństwa informacji i administratora systemu informatycznego oraz określić ich zakresy czynności.

 Gramm Technika Sp. z o.o. Karolewo 5 66-300 Międzyrzecz	POLITYKA BEZPIECZEŃSTWA		WYDANIE: I/2018	
	INSTRUKCJA - OCENA RYZYKA PRZETWARZANIA DANYCH			
	WPROWADZONO DNIA:		OBOWIĄZUJE OD:	

2.3. ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH


Do uprawnień i obowiązków Administratora Systemów Informatycznych należą w szczególności:

- a) Czynne wsparcie Gramm w administrowaniu Systemem Informatycznym, udział w ocenie ryzyka dla wolności i praw osób, których dane dotyczą, oraz jeżeli ocena tego wymaga, czynny udział w ocenie skutków dla ochrony danych osobowych, oraz na wniosek Administratora Danych dokonuje niezbędnych dodatkowych operacji mających na celu zabezpieczenie danych osobowych obsługiwanych w jego zakresie oraz ewentualne zminimalizowanie skutków utraty tych danych osobowych dla Organizacji i osób, których dane zostały utracone.
- b) Nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych.
- c) Nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów.
- d) Podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.
- e) Sprawuje nadzór nad wykonywaniem napraw, konserwacji oraz likwidacji urządzeń komputerowych i nośników danych, na których zapisane są dane osobowe na wniosek Administratora, bądź zgodnie z obowiązującym prawem lub wymaganiami przywołanymi w niniejszej polityce.

2.4. OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH


Osoby upoważnione do dysponowania, gromadzenia, przetwarzania, archiwizowania i niszczenia danych osobowych w Gramm są zobowiązane do przestrzegania zasad ochrony danych osobowych, a w szczególności do:

- a) Przetwarzania danych osobowych i ich ochrony w sposób zgodny z przepisami Ustawy, Rozporządzenia, Rozporządzenia o RODO, Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym.
- b) Przetwarzania danych osobowych wyłącznie w celu i zakresie ustalonym indywidualnie przez administratora danych w upoważnieniu i tylko w celu wykonywania nałożonych na nich obowiązków – odwołanie z funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych. Zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia lub odwołaniu z pełnionej funkcji.
- c) Zabezpieczają dane przed ich udostępnianiem osobom nieupoważnionym.
- d) Osoby upoważnione do zbierania, przechowywania, przetwarzania i dysponowania danymi osobowymi znajdują się w załączonej do polityki „**Ewidencji osób upoważnionych do przetwarzania danych osobowych**” – zał. nr 2, która jest nadzorowana przez Administratora Danych.
- e) Prawo do dysponowania, przechowywania, zbierania i przetwarzania oraz dysponowania danymi osobowymi pracownicy Gramm nabywają tylko po udzieleniu im zgody przez Administratora Danych na podstawie „**Indywidualnego upoważnienia do przetwarzania danych osobowych**”.

 Gramm Technika Sp. z o.o. Karolewo 5 66-300 Międzyrzecz	POLITYKA BEZPIECZEŃSTWA		WYDANIE: I/2018	
	INSTRUKCJA - OCENA RYZYKA PRZETWARZANIA DANYCH			
	WPROWADZONO DNIA:		OBOWIĄZUJE OD:	


3. INDYWIDUALNE UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Do przetwarzania danych osobowych, mogą być dopuszczone wyłącznie osoby posiadające imienne indywidualne upoważnienie do przetwarzania danych wydawane przez Administratora Danych, na podstawie aktualnego zakresu obowiązków, zgodnie ze wzorem określonym w załączniku nr 1 do Polityki bezpieczeństwa.
2. Administrator danych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych. Ewidencja sporządzana jest w wersji elektronicznej i papierowej oraz zawiera następujące informacje:
 - Imię i nazwisko osoby upoważnionej.
 - Datę nadania i ustania oraz jasno zdefiniowany zakres upoważnienia do przetwarzania danych osobowych.
 - Identyfikator, jeżeli dane są przetwarzane w systemie informatycznym umożliwiającym nadanie identyfikatora.
3. W przypadku zmiany zakresu czynności pracownika, do wykonywania których został upoważniony na mocy wydanego upoważnienia, administrator danych:
 - a) Opracowuje nowe upoważnienie do przetwarzania danych osobowych, jeśli zakres czynności uległ zmniejszeniu.
 - b) Przygotowuje aneks do wydanego upoważnienia do przetwarzania danych, jeśli zakres czynności uległ rozszerzeniu.
4. Każdy pracownik przed dopuszczeniem go do przetwarzania danych osobowych musi zostać przeszkolony przez Administratora Danych w zakresie przepisów dotyczących ochrony danych osobowych, ze szczególnym uwzględnieniem Rozporządzenia o RODO, oraz Polityki bezpieczeństwa i Instrukcji.

 Gramm Technika Sp. z o.o. Karolewo 5 66-300 Międzyrzecz	POLITYKA BEZPIECZEŃSTWA		WYDANIE: I/2018	
	INSTRUKCJA - OCENA RYZYKA PRZETWARZANIA DANYCH			
	WPROWADZONO DNIA:		OBOWIĄZUJE OD:	


4. UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator Danych osobowych może, na podstawie umowy powierzenia przetwarzania danych osobowych, przekazać dane innemu podmiotowi.
2. Przekazanie danych osobowych odbywa się wyłącznie na podstawie pisemnej umowy. Wzór umowy stanowi Załącznik nr 3 do Polityki Bezpieczeństwa.
3. Umowa powierzenia danych osobowych może być częścią umowy o współpracy z podmiotem zewnętrznym.
4. Dane powierza się wyłącznie podmiotowi, który spełnia wymagania ustawy o ochronie danych osobowych oraz wytyczne rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urzędnicy oraz systemy informatyczne, służące do przetwarzania danych osobowych, a także spełnia wymagania Rozporządzenia o RODO.
5. Przetwarzanie danych osobowych przez podmiot zewnętrzny może odbywać się wyłącznie w zakresie i celu przewidzianym w umowie.
6. Administrator Danych może upoważnić przedstawiciela podmiotu, któremu dane są powierzane, do nadania upoważnień do przetwarzania danych osobowych w jego imieniu, jeśli jest to niezbędne do realizacji postanowień współpracy.
7. Przedstawiciel podmiotu, któremu powierzono dane osobowe, powinien niezwłocznie poinformować administratora danych o przypadkach naruszenia bezpieczeństwa powierzonych danych osobowych i podjętych krokach w celu ich ponownego zabezpieczenia.
8. Przedstawiciel podmiotu, któremu powierzono dane osobowe powinien ściśle współpracować z Administratorem Danych w przypadku utraty powierzonych danych osobowych, w przypadku określania ryzyk związanych z przetwarzaniem danych, oraz podczas niezbędnych działań mających na celu poprawę bezpieczeństwa ochrony danych osobowych na rzecz Gramm – jeżeli jest to wymagane.
9. Administrator Danych ma prawo do kontroli podmiotu, któremu powierzono dane osobowe, w zakresie bezpieczeństwa przetwarzania powierzonych danych.

 Gramm Technika Sp. z o.o. Karolewo 5 66-300 Międzyrzecz	POLITYKA BEZPIECZEŃSTWA		WYDANIE: I/2018	
	INSTRUKCJA - OCENA RYZYKA PRZETWARZANIA DANYCH			
	WPROWADZONO DNIA:		OBOWIĄDUJE OD:	


5. OGÓLNE ZASADY BEZPIECZEŃSTWA OBOWIĄZUJĄCE PRZY PRZETWARZANIU DANYCH OSOBOWYCH

1. Za bezpieczeństwo przetwarzania danych osobowych w Gramm Technika sp. z o.o. odpowiedzialny jest V-ce Prezes, natomiast w określonych zbiorach, indywidualną odpowiedzialność ponoszą również pracownicy mający dostęp do tych danych.
2. Gramm Technika sp. z o.o. postępując zgodnie z wymaganiami prawnymi i wytycznymi Rozporządzenia o RODO określiła niezbędne minimum danych osobowych, którymi musi się posługiwać, w celu właściwego funkcjonowania organizacji, oraz w celu spełnienia wymagań prawnych ciążących na organizacji w związku z jej działalnością.
3. Organizacja w oparciu o własną instrukcję oceny ryzyka zał. nr 7 – przeprowadza ocenę ryzyka dla utraty danych osobowych przetwarzanych w organizacji.
4. Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
5. W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. „czystego biurka”. Zasada ta oznacza nie pozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Wszelkie dokumenty zawierające dane osobowe powinny być przechowywane w sposób jednoznacznie zabezpieczający je przed utratą. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników.
6. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów, zbędnych nośników zawierających dane osobowe musi odbywać się w sposób uniemożliwiający odczytanie zawartej w nich treści.
7. Niedopuszczalne jest wnoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.
8. Pracownicy zobowiązani są do nieudzielania informacji o danych osobowych innym podmiotom, chyba że obowiązek taki wynika wprost z przepisów prawa i tylko w sytuacji, gdy przesłanki określone w takich przepisach zostały spełnione.
9. Przebywanie osób nieuprawnionych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych, chyba że dane te są w odpowiedni sposób zabezpieczone przed dostępem.
10. Pracownicy zobowiązani są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe w czasie ich chwilowej nieobecności w pomieszczeniu pracy, jak i po jej zakończeniu, a klucze nie mogą być pozostawione

 Gramm Technika Sp. z o.o. Karolewo 5 66-300 Międzyrzecz	POLITYKA BEZPIECZEŃSTWA		WYDANIE: I/2018	
	INSTRUKCJA - OCENA RYZYKA PRZETWARZANIA DANYCH			
	WPROWADZONO DNIA:		OBOWIĄZUJE OD:	


w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia posiadanych kluczy przed nieuprawnionym dostępem.

11. Pracownicy, którzy podczas wykonywania obowiązków przetwarzają dane za pomocą urządzeń komputerowych, mają obowiązek każdorazowo przed opuszczeniem miejsca pracy (komputer) do wylogowania się, tak aby nikt inny nie był w stanie skorzystać z ich dostępu do danych osobowych.
12. Pracownicy na wniosek Administratora Danych uzyskują od Administratora Systemu Informatycznego dostęp do danych osobowych zgodnie z zaleceniami Administratora i tylko w zakresie opisanym w Indywidualnym upoważnieniu do przetwarzania danych osobowych.
13. Pracownicy zobowiązani są do niezwłocznego zawiadamiania administratora danych o wszelkich przypadkach naruszenia bezpieczeństwa danych osobowych, a także o przypadkach utraty lub kradzieży dokumentów lub innych nośników zawierających te dane osobowe.
14. Administrator Danych po powzięciu wiadomości o utracie danych osobowych, które mogą mieć istotny wpływ na bezpieczeństwo osób, których dane zostały utracone, informuje właściwy organ nadzorczy o ile to możliwe w terminie nie przekraczającym 72 godzin.
15. Administrator Danych w przypadku utraty istotnych danych osobowych (mogących mieć wpływ na bezpieczeństwo danej osoby) niezwłocznie – kiedy to tylko możliwe – informuje daną osobę o zakresie utraty danych, o jego działaniach i ewentualnie działaniach koniecznych do powzięcia przez osobę, której dane zostały utracone.
16. Pracownicy, oraz Interesanci których dane osobowe są przetwarzane w Gramm mają prawo każdorazowo – jeżeli jest to uzasadnione – do otrzymania informacji dotyczących ich danych i ich sposobu przetwarzania oraz zabezpieczania. Wszyscy, których dane osobowe są przetwarzane w Gramm mają prawo do wprowadzania zmian w swoich danych – o ile jest to zasadne – oraz, o ile wykażą zgodność nowych danych z rzeczywistością.
17. Wszyscy, których dane osobowe są przetwarzane w Gramm mają prawo do „bycia zapomnianymi”, co również oznacza, że mogą cofnąć swoją zgodę na przetwarzanie danych osobowych przez Gramm – w każdej chwili.
18. Organizacja Gramm zobowiązuje się do umożliwienia wszystkim, których dane osobowe są przetwarzane w organizacji do bycia zapomnianym – usunięcie danych osobowych, zaprzestanie przetwarzania danych osobowych na żądanie osoby fizycznej, chyba że istnieją inne przesłanki np. prawne (współpraca z organami ścigania, obowiązek archiwizacji danych, współpraca z organami państwowymi wynikająca z postanowień prawa i obowiązków Organizacji w stosunku do prawodawcy), aby dane osobowe nie zostały usunięte.
19. Organizacja Gramm ma obowiązek poinformowania osób fizycznych w przypadku utraty ich danych. Organizacja Gramm musi jak najszybciej bez zbędnej zwłoki poinformować osobę fizyczną, której dane utraciła o rozmiarze tego zdarzenia, o rodzaju danych jakie zostały utracone, oraz o działaniach podjętych w związku z tym, a także o zaleceniach dla osoby, której dane zostały utracone.

 Gramm Technika Sp. z o.o. Karolewo 5 66-300 Międzyrzecz	POLITYKA BEZPIECZEŃSTWA		WYDANIE: I/2018	
	INSTRUKCJA - OCENA RYZYKA PRZETWARZANIA DANYCH			
	WPROWADZONO DNIA:		OBOWIĄZUJE OD:	


6. INSTRUKCJA POSTĘPOWNIA W SYTUACJI NARUSZENIA ZASAD OCHRONY DANYCH OSOBOWYCH

1. W przypadku stwierdzenia, przez osobę przetwarzającą dane osobowe lub jej przełożonego, zaistnienia lub podejrzenia zaistnienia naruszenia bezpieczeństwa lub/i zasad ochrony danych osobowych, osoby te są zobowiązane natychmiast zawiadomić o tym Administratora Danych, a w przypadku gdy naruszenie dotyczy danych w systemie informatycznym, także administratora systemu informatycznego.
2. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Danych lub upoważnionej przez niego osoby, osoba powiadamiająca powinna:
 - a) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków, a następnie ustalić przyczyny lub sprawców zaistniałego zdarzenia, jeżeli jest to możliwe,
 - b) zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,
 - c) udokumentować wstępnie zaistniałe naruszenie w „**Rejestrze naruszeń ochrony danych osobowych**” – zał. nr 8
 - d) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Danych lub osoby upoważnionej.
3. Administrator Danych, w obecności osoby, która stwierdziła naruszenie zabezpieczeń lub zasad ochrony danych osobowych – przeprowadza oględziny miejsca stwierdzenia naruszenia. Jeżeli Administrator Danych potwierdzi naruszenie danych osobowych, podejmuje natychmiastowe kroki w celu dokonania oceny zagrożenia dla osoby, bądź osób fizycznych których to naruszenie bezpieczeństwa dotyczy. Jeżeli naruszenie danych osobowych jest poważne i zagraża bezpieczeństwu fizycznemu, lub innemu osób fizycznych, których dane zostały naruszone – Administrator Danych natychmiast powiadamia te osoby. Ponadto w takim przypadku Administrator Danych ma obowiązek powiadomić również organ nadzorczy w czasie nie dłuższym niż 72 godziny od stwierdzenia poważnego naruszenia bezpieczeństwa danych osobowych.
4. Powiadomienie osoby fizycznej, o którym mowa w ust. 3 powinno zawierać w szczególności:
 - a) Wskazanie terminu stwierdzenia naruszenia ochrony danych, o ile to możliwe.
 - b) Określenie szkód i zagrożenia dla danych przetwarzanych w stosunku do osoby których dane są zagrożone.
 - c) Poinformowanie osób fizycznych, których dane zostały utracone o charakterze i rozmiarze zagrożenia, o podjętych ewentualnych działaniach i zaleceniach dla tych osób jeżeli takie istnieją.
5. Administrator Danych dokonuje analizy i oceny całokształtu stwierdzonego naruszenia zasad ochrony danych osobowych, a następnie zarządza wprowadzenie środków eliminujących w przyszłości podobne zdarzenia.
6. W przypadku stwierdzenia ewidentnego naruszenia dyscypliny pracy przez osobę zatrudnioną przy przetwarzaniu danych osobowych, administrator danych podejmuje stosowne środki dyscyplinujące.

 Gramm Technika Sp. z o.o. Karolewo 5 66-300 Międzyrzecz	POLITYKA BEZPIECZEŃSTWA		WYDANIE: I/2018	
	INSTRUKCJA - OCENA RYZYKA PRZETWARZANIA DANYCH			
	WPROWADZONO DNIA:		OBOWIĄZUJE OD:	

7. POSTANOWIENIA KOŃCOWE

1. Wszelkie zmiany w Polityce bezpieczeństwa wymagają zatwierdzenia przez Administratora Danych.
2. Integralną część Polityki bezpieczeństwa stanowią załączniki do niniejszego dokumentu.
3. Aktualizacja załączników do Polityki bezpieczeństwa dokonywana będzie w miarę potrzeb.
4. Odpowiedzialność karną za przetwarzanie danych osobowych niezgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. 2015 poz. 2135), oraz przepisami wykonawczymi do tej ustawy określają przepisy art. 49-54 ww. ustawy.
5. Rozporządzenie o RODO określa zasady ewentualnej odpowiedzialności finansowej przedsiębiorstw i osób fizycznych za naruszenie zasad Rozporządzenia o RODO.
6. Osoby, które zostały zapoznane z Polityką bezpieczeństwa zobowiązane są do bezwzględnego stosowania zasad w niej zawartych (oświadczenie o bezwzględnym stosowaniu zapisów Polityki bezpieczeństwa zawarte zostało w indywidualnym upoważnieniu do przetwarzania danych osobowych).
7. Upoważnienia do przetwarzania danych osobowych przechowywane są w aktach personalnych pracowników.
8. Wszystkie regulacje określone w Polityce bezpieczeństwa dotyczą przetwarzania danych osobowych w bazach Gramm Technika prowadzonych zarówno w formie elektronicznej, jak i w formie papierowej.
9. W przypadku konieczności udostępnienia danych osobowych, Administrator danych udostępnia posiadane w zbiorze dane osobowe, osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
10. Dane osobowe udostępnia się na pisemny wniosek, chyba że przepis innej ustawy stanowi inaczej.
11. Udostępnione dane osobowe można wykorzystywać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

 Gramm Technika Sp. z o.o. Karolewo 5 66-300 Międzyrzecz	POLITYKA BEZPIECZEŃSTWA		WYDANIE: I/2018	
	INSTRUKCJA - OCENA RYZYKA PRZETWARZANIA DANYCH			
	WPROWADZONO DNIA:		OBOWIĄZUJE OD:	

8. ZAŁĄCZNIKI

Załącznik nr 1 – Wzór **Indywidualne upoważnienie do przetwarzania danych osobowych**

Załącznik nr 2 – Wzór **Ewidencja osób upoważnionych do przetwarzania danych osobowych**

Załącznik nr 3 – Wzór **Umowa powierzenia przetwarzania danych osobowych**

Załącznik nr 4. **Wykaz podmiotów, którym Administrator Danych powierzył przetwarzanie danych osobowych**

Załącznik nr 5: **Wykaz urzędzeń w organizacji, na których przetwarzane są dane osobowe**

Załącznik nr 6 – **Arkusz identyfikacji przetwarzania danych osobowych, wykaz zbiorów danych przetwarzanych**

Załącznik nr 7 – **Instrukcja oceny ryzyka przetwarzania danych osobowych**

Załącznik nr 8 – Wzór **Rejestr naruszeń ochrony danych osobowych**

Załącznik nr 9 – **Instrukcja zarządzania systemem informatycznym**