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

GRAMM TECHNIKA SP. Z O.O.

KAROLEWO 5

66-300 MIĘDZYRZECZ

Data i miejsce sporządzenia dokumentu:	Karolewo 28/03/2018
Ilość stron:	

SPIS TREŚCI

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 prywatność i godność 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 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.

1.3. TERMINY ZASTOWOSANE W POLITYKI BEZPIECZEŃSTWA

Podstawowe terminy użyte w Polityce bezpieczeństwa i ich znaczenia:

1. ustawa – ustawę 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 - 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).
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 organizacja 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.

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 – jakiekolwiek 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.

2. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

2.1. INFORMACJE OGÓLNE

1. Osoby odpowiedzialne za dostęp i przetwarzanie danych w Organizacji Gramm, są zobowiązane do przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami Ustawy, Rozporządzenia, Rozporządzenia RODO i Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemami informatycznymi.

2. Osobami odpowiedzialnymi za przetwarzanie danych osobowych w Gramm Technika są:
   a) Administrator Danych,
   b) Administrator Systemów Informatycznych,
   c) Osoby upoważnione, w tym osoby i instytucje upoważnione na mocy umowy z Gramm o dostępie, administrowaniu i zarzadzaniu danymi osobowymi na określone jasno sprecyzowane cele.

3. 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.

4. 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

1. Administrator danych Gramm Technika Sp. z o.o., zwany dalej Gramm – reprezentowany przez V-ce Prezesa Zarządu

2. Administrator danych:

   a) 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, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
   b) 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
   c) upoważnia poszczególne osoby do przetwarzania danych osobowych w indywidualnym zakresie, odpowiadającym zakresowi ich zadań i obowiązków, w oparciu o załącznik **„Arkusz identyfikacji przetwarzania danych osobowych, wykaz zbiorów danych przetwarzanych**” –

zał. nr 6, 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 nadzorczemu 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, które dane dotyczyły,
i) 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

3. Administrator danych może powołać administratora bezpieczeństwa informacji i administratora systemu informatycznego oraz określić ich zakresy czynności.

2.3. ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

1. Administratorem Systemów Informatycznych jest na mocy „Umowa powierzenia przetwarzania danych osobowych" AMP SYSTEM CHAŁUPKA Spółka Jawna z siedzibą w Gorzowie Wielkopolskim.

2. 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 bierze 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,
   c) zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia lub odwołaniu z pełnionej funkcji,
   d) zabezpieczają dane przed ich udostępnianiem osobom nieupoważnionym.

e) Osoby upoważnione do zbierania, przechowywania, przetwarzania i dysponowania danymi osobowymi znajdują się w załączonej do polityki **Ewidencja osób upoważnionych do przetwarzania danych osobowych** – zał. nr 2, która jest nadzorowana przez Administratora Danych.

f) 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.**

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 papierowej i 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.

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 urządzenia 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 dotyczących wdrażania działań dla poprawy bezpieczeństwa ochrony danych osobowych na rzecz Gramm znajduje się w dokumencie **Wykaz podmiotów, którym Administrator Danych powierzył przetwarzanie danych osobowych** – zał. nr 4
9. Administrator Danych ma prawo do kontroli podmiotu, któremu powierzono dane osobowe, w zakresie bezpieczeństwa przetwarzania powierzonych danych.

5. OGÓLNE ZASADY BEZPIECZEŃSTWA OBOWIĄZUJĄCE PRZY PRZETWARZANIU DANYCH OSOBOWYCH

1. Za bezpieczeństwo przetwarzania danych osobowych w Gramm Technika sp. z o.o. ponosi V-ce Prezes, natomiast w określonych zbiorach, indywidualną odpowiedzialność ponoszą również pracownicy mający dostęp do tych danych.

2. Organizacja Gramm 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 z celu spełnienia wymagań prawnych ciążących na organizacji w związku z jej działalnością.

3. Organizacja w oparciu o własną instrukcję oceny ryzyka zał. nr

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 wynoszenie 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 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 danych istotnych danych osobowych (mogących mieć wpływ na bezpieczeństwo danej osoby) niezwłocznie – jak 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.

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 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) datę, godzinę i miejsce rozpoznania sytuacji
   b) precyzyjne wskazanie stwierdzonego naruszenia zasad związanych z ochroną przetwarzania danych osobowych lub zabezpieczeń stosowanych w tym zakresie w systemie informatycznym, gdzie przetwarzane są dane, lub poza systemem informatycznym,
   c) wskazanie terminu stwierdzenia naruszenia ochrony danych, o ile to możliwe
   d) określenie szkód i zagrożenia dla danych przetwarzanych w stosunku do osoby których dane są zagrożone
   e) poinformowanie osób fizycznych, których dane zostały utracone o charakterze i rozmiarze zagrożenia, o podjętych ewentualnych działaniach i zaleceniach dla tych osób jeżeli takie istnieją
   f) podpisy osób obecnych przy oględzinach.

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.

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.

Dokument sporządzono:	**Pełen podpis Administratora Danych:**	**Pieczęć**
Data: …/…/…… (dd/mm/rrrr) Miejsce: ……		

8. ZAŁĄCZNIKI

Załącznik nr 1– Wzór **Indywidualne upoważnienia 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 urządzeń w organizacji, na których przetwarzane są dane osobowe**

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

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

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

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

Dokument sporządzono:	**Pełen podpis Administratora Danych:**	**Pieczęć**
Data: …/…/…… (dd/mm/rrrr) Miejsce: ……		

Załącznik nr 1 Indywidualne upoważnienie do przetwarzania danych osobowych

INDYWIDUALNE UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Z dniem _____ upoważniam Panią / Pana do przetwarzania danych osobowych, administrowanych lub/i powierzonych do przetwarzania Administratorowi, w postaci papierowej oraz w ramach nadanych dostępów do systemów informatycznych, zgodnie z zajmowanym stanowiskiem jak w tabeli poniżej

Imię i nazwisko i stanowisko upoważnionego pracownika	
Zbiory danych objęte zakresem upoważnienia	

Jednocześnie zgodnie z nadanym upoważnieniem, zobowiązuje Panią / Pana do przestrzegania przepisów dotyczących ochrony danych osobowych oraz wprowadzonych i wdrożonych do stosowania przez Administratora postanowień Polityki Bezpieczeństwa oraz związanych dokumentów.

Niniejsze upoważnienie traci swoją moc:

Najpóźniej z dniem odwołania albo rozwiązania lub wygaśnięcia umowy o pracę, umowy zlecenia, umowy o dzieło, lub innej umowy cywilnoprawnej łączącej Pana / Panią z Administratorem

_____ _____

Miejscowość i data *(z upoważnienia Administratora Danych)*

OŚWIADCZENIE

Oświadczam, że zostałem zapoznany z przepisami dotyczącymi ochrony danych osobowych w szczególności ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. 2016 poz. 922 z późn. zm.), wydanych na jej podstawie aktów wykonawczych, a także z Rozporządzeniem 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), oraz wprowadzonej i wdrożonej do stosowania Polityki Bezpieczeństwa wraz ze związanymi dokumentami.

Zobowiązuje się do:

- Zachowania w tajemnicy danych osobowych, do których mam, lub będę miał/a dostęp w związku z wykonywaniem zadań służbowych i obowiązków pracowniczych
- Niewykorzystywania danych osobowych w celach pozasłużbowych o ile nie są one jawne

- Zachowania w tajemnicy sposobu zabezpieczenia danych osobowych
- Korzystania ze sprzętu IT oraz oprogramowania wyłącznie w związku z wykonywaniem obowiązków
- Wykorzystywania jedynie legalnego oprogramowania pochodzącego od Administratora Danych
- Należytej dbałości o sprzęt i oprogramowanie zgodnie z dokumentacją przetwarzania danych osobowych
- Nieudostępniania sprzętu służbowego osobom trzecim
- Korzystania z urządzeń i komputerów przenośnych zgodnie z zasadami przetwarzania danych osobowych

Przyjmuję do wiadomości, że postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane przez Pracodawcę za ciężkie naruszenie obowiązków pracowniczych i w rozumieniu art. 52. § 1 pkt 1 Kodeksu Pracy lub za naruszenie przepisów karnych ww. Ustawy o ochronie danych osobowych, lub naruszeniem przepisów Rozporządzenia o RODO.

Podpis osoby upoważnionej

Załącznik nr 2 – Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Nr	Imię i nazwisko osoby upoważnionej	Data nadania upoważnienia	Data ustania upoważnienia	Indywidualny identyfikator w systemie informatycznym	Nazwy zbiorów objętych zakresem upoważnienia
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					

Załącznik nr 3 – Umowa powierzenia przetwarzania danych

Umowa powierzenia przetwarzania danych osobowych
zawarta dnia _____ pomiędzy:
(zwana dalej „Umową")

_____ *(*dane podmiotu który umowę zawiera)*

zwany w dalszej części umowy **„Podmiotem przetwarzającym"**
reprezentowana przez:
_____

oraz

_____ *(*dane podmiotu który umowę zawiera)*

zwany w dalszej części umowy **„Administratorem danych" lub „Administratorem"**
reprezentowana przez:
_____

§ 1
Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. (zwanego w dalszej części „Rozporządzeniem") dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.

§2
Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie umowy dane (**należy podać rodzaj danych*) …… *np. dane zwykłe oraz dane szczególnych kategorii ……. (*należy podać kategorię osób, których dane dotyczą) np. pracowników administratora, klientów administratora itd. w postaci …….. np. imion i nazwisk, adresu zamieszkania, nr PESEL itd.*
2. Powierzone przez Administratora danych, dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu …….. (**należy podać cel przetwarzania danych przez podmiot przetwarzający*) *np. realizacji umowy z dnia …… nr …… w zakresie prowadzenia kadr.*

§3
Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.

2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.

3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.

4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.

5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa/ zwraca Administratorowi wszelkie dane osobowe (*należy wybrać czy podmiot przetwarzający ma usunąć czy zwrócić dane*) oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.

6. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.

7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi w ciągu ….. (**można wskazać np. w ciągu 24 h*).

§4
Prawo kontroli

1. Administrator danych zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.

2. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum …….. *(*należy wpisać z ilu dniowym wyprzedzeniem Administrator informuje o kontroli*) jego uprzedzeniem.

3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni (**administrator termin może określić dowolnie*).

4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§5
Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora danych.

2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.

3. Podwykonawca, o którym mowa w §3 ust. 2 Umowy winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.

4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 6
Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.

2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Generalnego Inspektora Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

§7
Czas obowiązywania umowy

1. Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas *nieokreślony/określony* od ….. do ….. .*

2. Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem …… * okresu wypowiedzenia.

§8
Rozwiązanie umowy

1. Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy Podmiot przetwarzający:

   a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;

   b) przetwarza dane osobowe w sposób niezgodny z umową;

   c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych;

§9
Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne").
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

§10
Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy Administratora danych (**lub Podmiotu przetwarzającego w zależności od postanowień stron*).

_____ _____

Administrator danych Podmiot przetwarzający

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

	Adres / lokalizacja	Uwagi
Podmioty, którym Administrator Danych powierzył przetwarzanie danych osobowych	**AGAW Usługi BHP Agnieszka Woźniak, Poznańska 109/38a/3 66 – 300 Międzyrzecz**	
	AMP SYSTEM CHAŁUPKA Spółka Jawna, Drzymały 39/5 66-400 Gorzów Wielkopolski	
	Grupa 24 – Ochrona mienia Piotrowscy, Aleja Wojska Polskiego 37 65-784 Zielona Góra	

Załącznik nr 5. Wykaz urządzeń w organizacji, na których przetwarzane są dane osobowe

Lp.	Nr inwent.	Nazwa środka trwałego	Lokalizacja	Nr fabryczny	Zakup
Nr K-23	37/2009	Zestaw komputerowy	Produkcja WOCH		31.12.2009
Nr K-24	38/2009	Zestaw komputerowy	Produkcja WA		31.12.2009
Nr K-34	51/491	Zestaw komputerowy	Laboratorium		30.09.2012
Nr K-36	55/491	Laptop - Notebook - DELL	Dział Techniczny		20.09.2014
Nr K-37	1/03/15	Laptop - Notebook - ACER	Automatyk		19.03.2015
Nr K-39	1/09/15	Laptop - Notebook - ASUS	Kierownik Produkcji		21.09.2015
Nr K-44	2/09/16	Zestaw komputerowy	Kadry		29.09.2016
Nr K-49	1/02/17	Laptop - Notebook - DELL	Automatyk		07.02.2017
Nr K-56	1/12/17	Zestaw komputerowy	Księgowość		07.12.2017
Nr K-57	2/12/17	Serwer - kasa	Kasa		07.12.2017
Nr K-58		Laptop - Notebook - HP	Zarząd		20.09.2014
Nr K-59		Zestaw komputerowy	Kontrola Jakości		10.07.2017
Nr K-60		Tel. komórkowy- Honor tel. 601 811 510	Zarząd		
Nr K-61		Karta sim nr tel. 605 831 874	Zarząd		
Nr K-62		Tel. komórkowy - Honor tel. 691 412 717	Kierownik Produkcji		
Nr K-63		Tel. komórkowy - Honor tel. 661 552 408	Kadry		

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

NAZWA ZBIORU DANYCH	OBSZAR PRZETWARZANIA	KATEGORIE DANYCH	SPOSÓB PRZETWARZANIA	ZAKRES DANYCH I CEL PRZETWARZANIA
Zbiór Kadrowo – Płacowy	Dział kadr, Dział Księgowości , Dział Jakości Gramm Technika Sp. z o.o. Karolewo 5 66-300 Międzyrzecz	Pracownicy Organizacji Gramm Technika	- Microsoft Office, - Comarch – ERP Optima, - Lider KP – Kadry, Płace, - Płatnik – ZUS - Zbiór przetwarzany w postaci papierowej, - E-deklaracje,	Imię i nazwisko, nazwa miejsce pracy i funkcja, lub stanowisko, seria i nr dowodu osobistego, data i miejsce urodzenia, adres zameldowania i zamieszkania, płeć, imiona rodziców, stan rodzinny, imię i nazwisko i data urodzenia współmałżonka, data urodzenia dziecka, lub dzieci pracownika, imię i nazwisko i nr tel. osoby którą należy poinformować w razie wypadku, czas pracy, przebieg kariery, wysokość wynagrodzenia, nagrody, premie, informacje o zatrudnieniu u poprzedniego pracodawcy, informacje o NFZ, informacje o Urzędzie Skarbowym, poziom wykształcenia, rok ukończenia i rodzaj szkoły, typ i profil ukończonej szkoły, specjalizacja, ukończone studia podyplomowe, ukończone kursy i posiadane dodatkowe uprawnienia, umiejętności, znajomość języków obcych , poziom obsługi komputera, prawo jazdy, zainteresowania, nr rachunku bankowego, nazwa banku w którym prowadzony jest rachunek bankowy, rozmiar odzieży roboczej, obuwia ochronnego, wyniki testów i egzaminów wewnętrznych, listy obecności na szkoleniach wewnętrznych – dane zawarte z tym zbiorze podlegają przetwarzaniu w dziale Kadr, celem przetwarzania tych

				danych jest rozwój pracowników, spełnienie wymagań prawnych dotyczących świadczeń pracowniczych pracowników organizacji, przetwarzanie danych jest niezbędne do wypełnienia obowiązków prawnych ciążących na Administratorze Danych
Zbiór rekrutacje	Dział Kadr, Dział Techniczny, V-ce Prezes Gramm Technika Sp. z o.o. Karolewo 5 66-300 Międzyrzecz	Kandydaci na pracowników	- Microsoft Office, - Zbiór przetwarzany w postaci papierowej,	Imiona i nazwiska, data urodzenia, obywatelstwo, miejsce zamieszkania, adres do korespondencji, wykształcenie, nazwa szkoły, data ukończenia, tytuł zawodowy, kursy, ukończone studia, dodatkowe uprawnienia, zainteresowania, umiejętności – celem gromadzenia i przechowywania tych danych jest rekrutacja pracowników do Organizacji Gramm Technika, na potrzeby gromadzenia i przetwarzania danych dla potrzeb rekrutacji kandydaci wyrażają swoją zgodę na te działania na dokumentach rekrutacyjnych CV – poprzez dodanie do CV klauzuli – „Wyrażam zgodę na przetwarzanie moich danych osobowych dla potrzeb niezbędnych do realizacji procesu rekrutacji (zgodnie z Ustawą z dnia 29 sierpnia 1997 roku O ochronie danych osobowych; tekst jednolity: Dz. U. z 2002r. Nr 101, poz. 926 ze zm.), oraz zgodnie z Rozporządzeniem RODO”
Kontrahenci,	Dział Kadr i Płac, Dział Księgowości	Pracownicy Kontrahentów i kontrahenci	- Microsoft Office, - Zbiór przetwarzany w postaci papierowej	Imię nazwisko, adres, numer telefonu, e-mail, nazwa zakładu pracy, NIP, - celem gromadzenia tych danych jest – niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez

				administratora, lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesu, lub podstawowe wolności i prawa osoby, której dane dotyczą, wymagające ochrony danych osobowych
Korespondencja przychodząca i wychodząca	Dział Kadr i Płac, Dział Księgowości	Dane adresowe korespondencji	- Zbiór przetwarzany w postaci papierowej	Imię nazwisko, nazwa i adres osoby, korespondującej z organizacją

Załącznik nr 8 – Wzór - Rejestr naruszeń danych osobowych

L.p.	Data naruszenia	Godzina naruszenia	Kategoria osób, których dane naruszono	Liczba osób	Liczba wpisów	Dane inspektora ODO / punkt kontaktowy	Dane organu nadzorczego	Czy zawiadomiono organ?	Czy zawiadomiono osoby?	Powód zwolnienia z zawiadomienia osoby
						Gramm Technika Sp. z o.o. Karolew 5, 66-300 Międzyrzecz	Biuro Generalnego Inspektora Ochrony Danych Osobowych ul. Stawki 2 00-193 Warszawa			

Załącznik nr 9 – Instrukcja zarządzania systemem informatycznym

Cel i zakres zastosowania instrukcji

Instrukcja określa sposób zarządzania systemem informatycznym, wykorzystywanym do ochrony, gromadzenia, przesyłania i przetwarzania danych osobowych przez administratora danych – w celu zabezpieczenia tych danych przed nieupoważnionym dostępem osób trzecich, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem. Instrukcja obejmuje swoim zakresem wszystkie osoby biorące udział w przetwarzaniu danych w Gramm, oraz na rzecz Gramm.

POSTANOWIENIA OGÓLNE

- Instrukcja została opracowana zgodnie z wymaganiami § 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych
- Instrukcja została opracowana również w oparciu o wymagania Rozporządzenia 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).
- Administrator Danych – Gramm Technika Sp. z o.o. w Karolewie 5 – posiada wszelkie uprawnienia do nadzorowania systemów informatycznych gwarantujące skuteczne realizowanie postanowień przywołanych powyżej rozporządzeń, co nie oznacza, że ma automatyczny dostęp do przetwarzanych w tych systemach danych .

DEFINICJE

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 – zgodnie z umową powierzenia przetwarzania danych jest to organizacja AMP SYSTEM CHAŁUPKA Spółka Jawna z siedzibą w Gorzowie Wielkopolskim.

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.

Hasło – ciąg znaków literowych, cyfrowych lub innych, znanych jedynie osobie upoważnionej do pracy w systemie informatycznym,

Osoba upoważniona – osoba, która została pisemnie upoważniona przez administratora danych do przetwarzania danych osobowych, na podstawie Indywidualnego upoważnienia do przetwarzania danych osobowych, które określa zakres i cel oraz czas trwania upoważnienia

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

Rejestr naruszeń ochrony danych osobowych – rejestr sporządzony do dokumentowania ewentualnych naruszeń ochrony danych osobowych przechowywany w dziale Kadr i Płac w siedzibie Gramm Technika w Karolewie 5 – w szafie zamykanej na klucz.

Rozliczalność danych – rozumie się przez to właściwość podmiotu zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi

Sieć publiczna – rozumie się przez to sieć publiczna w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 roku – prawo telekomunikacyjne

Sieć telekomunikacyjna – rozumie się przez to sieć telekomunikacyjną w rozumieniu . 2 pkt 23 ustawy z dnia 21 lipca 2000 roku – prawo telekomunikacyjne

System informatyczny Administratora Danych – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych.

Uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu

Użytkownik – osoba upoważniona do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło

Obowiązki administratora systemu:
- operacyjne zarządzanie systemami informatycznymi w sposób zapewniający ochronę danych osobowych
- przestrzeganie procedur i Polityki Bezpieczeństwa Administratora Danych
- kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną, oraz kontrola działań inicjowanych z sieci publicznej
- zarządzanie stosowanymi środkami uwierzytelniania, w tym rejestrowanie i wyrejestrowywanie użytkowników, oraz dokonywanie zmian uprawnień, na podstawie wniosków zatwierdzonych przez Administratora Danych
- utrzymanie systemu w sprawności technicznej

Regularne tworzenie kopii zapasowych zasobów danych osobowych oraz programów służących do ich przetwarzania, kresowe sprawdzanie poprawności wykonania kopii zapasowych
Wykonywanie, lub nadzór nad okresowymi przeglądami i konserwacją sprzętu IT, systemów informatycznych, aplikacji i elektronicznych nośników informacji,

Obowiązki użytkownika:
- przestrzeganie opracowanych dla systemu zasad i procedur przetwarzania danych
- przestrzeganie opracowanych dla systemu procedur operacyjnych i bezpieczeństwa
- udostępniane danych osobowych tylko osobom upoważnionym, lub uprawnionym do ich uzyskania

- uniemożliwienie dostępu do danych osobowych osobom nieuprawnionym
- natychmiastowe informowanie Administratora Danych i Administratora Systemu Informatycznego o wszelkich zauważonych naruszeniach bezpieczeństwa danych osobowych, bądź o podejrzeniu naruszenia bezpieczeństwa danych oraz wszelkich nieprawidłowościach w sposobie przetwarzania danych
- wykonywanie poleceń Administratora Danych w zakresie ochrony danych jeżeli nie sąone niezgodne z prawem.

Poziom bezpieczeństwa

Gramm Technika znając treść danych osobowych oaz respektując wymagania prawne w tym zakresie a w szczególności Rozporządzenie RODO postanawia wprowadzić „wysoki poziom" bezpieczeństwa w organizacji.

Eksploatacja systemów

Organizacja w celu wprowadzenia wysokiego poziomu zabezpieczeń danych osobowych postawania o wdrożeniu następujących zasad:
- użytkownikom zabrania się samodzielnego wprowadzania zmian w oprogramowaniu, sprzęcie informatycznym oraz samodzielnego konfigurowania tego oprogramowania i sprzętu
- zabrania się umożliwienia osobom trzecim dostępu do systemów informatycznych
- użytkownikom zabrania się we własnym zakresie instalowania nowego lub aktualizowania już zainstalowanego oprogramowania
- zabrania się korzystać z systemów informatycznych do celów innych niż wykonywanie obowiązków służbowych
- nie wolno podejmować prób testowania, modyfikacji i naruszania zabezpieczeń systemów informatycznych
- informacje przetwarzane muszą być zapisywane na dyskach serwera
- wszystkie aplikacje sieciowe, oraz współdzielone zasoby również muszą być zapisywane na dysku serwera
- użytkownikom nie wolno bez zgody Administratora Systemu Informatycznego, lub bez zgody Administrator Danych przenosić aplikacji oraz zasobów zlokalizowanych na serwerze, na dyski lokalne oraz przenośne nośniki danych
- bez zgody Administratora Danych zabronione jest podłączanie własnego, lub strony trzeciej urządzenia teleinformatycznego do systemu Gramm Technika Sp. z o.o. w Karolewo 5.

Nadawanie i odbieranie uprawnień do przetwarzania danych w Gramm

1. Użytkownicy nabywają uprawnienia do dostępu do danych osobowych w Gramm tylko na podstawie Indywidualnego upoważnienia do przetwarzania danych osobowych wydawanego przez Administratora Danych
2. Użytkownicy przed przystąpieniem do pracy z danymi osobowymi zobowiązani są do zapoznania się z niniejszą instrukcją, z Rozporządzeniem 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), Ustawą z dnia 29 sierpnia 1997 o ochronie danych (Dz.U z 2002 Nr 101, poz. 926 z późn. zm.
3. Pierwsze nadanie uprawnień dla użytkownika odbywa się po:
    - Uzyskaniu Indywidualnego upoważnienia

4. Zakres dostępu Użytkownika jest opisany w Indywidualnym Upoważnieniu i tylko do takiego zakresu Użytkownik ma dostęp
5. Administrator Systemu ma obowiązek przekazywać nadane hasła Użytkownikowi w sposób bezpieczny, tak aby nie zostały one użyte przez osoby trzecie
6. Administrator Danych może nadać uprawnienia do przetwarzania danych tymczasowo zewnętrznemu dostawcy, za pomocą Umowy powierzenia przetwarzania danych, bądź za pomocą Indywidualnego upoważnienia, jeżeli zewnętrzny dostawca usługi czasowo dokonuje przetwarzania danych na rzecz Gramm.
7. Dostęp do systemu powinien być możliwy tylko po podaniu indywidualnego identyfikatora i hasła
8. Dostęp do systemu i przetwarzania danych w systemie może uzyskać tylko osoba uprawniona przez Administratora Danych na podstawie Indywidualnego upoważnienia, które określa zakres danych do których osoba ta ma dostęp.
9. Rejestracja użytkownika polega na nadaniu identyfikatora i przydzieleniu jednorazowego hasła, oraz wprowadzenia tych danych do bazy użytkowników systemu, Użytkownik przy pierwszym logowaniu powinien dokonać zmiany hasła na nowe znane tylko jemu
10. Użytkownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora,
11. Użytkownik ma prawo do wykonywania tylko tych czynności na danych do których został upoważniony
12. Przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako naruszenie podstawowych uprawnień pracowniczych
13. Pracownik zatrudniony przy przetwarzaniu danych zobowiązany jest do zachowania tajemnicy, która obowiązuje go również po ustaniu stosunku pracy
14. Administrator Danych informuje Administratora systemu o każdej zmianie dotyczącej pracowników mającej wpływ na zakres uprawnień w systemie informatycznym

Odbieranie uprawnień i wyrejestrowanie

1. Wyrejestrowania Użytkownika z systemu informatycznego dokonuje administrator systemu na wniosek Administratora Danych
2. Wyrejestrowanie następuje poprzez
    - Zablokowanie konta użytkownika
    - Usunięcie danych użytkownika z bazy danych użytkowników

Metody i środku uwierzytelniania

1. Identyfikator nadawany jest zgodnie z procedurami Administratora Systemu
2. Każdy Użytkownik otrzymuje indywidualny identyfikator
3. Po odebraniu dostępu Użytkownikowi jego identyfikator nie może ponownie być użyty przez Administratora
4. Identyfikator i zakres dostępu Użytkownika jest rejestrowany w ewidencji osób upoważnionych do dostępu do danych
5. Hasło powinno składać się z unikalnego zestawu co najmniej 8 znaków zawierać małe i wielkie litery, oraz cyfry lub znaki specjalne, nie może być identyczne jak identyfikator
6. Użytkownicy powinni używać hasła łatwe do zapamiętania, ale trudne do odgadnięcia

7. System powinien wymuszać zmianę hasła co 90 dni,
8. Należy unikać używania cyklicznie tych samych haseł
9. Zabrania się użytkownikom udostępniania identyfikatorów i haseł innym osobom nieupoważnionym do dostępu do danych osobowych
10. Użytkownicy są odpowiedzialni za zachowanie poufności swoich haseł
11. Zabrania się przechowywać hasło w widocznym miejscu
12. Należy wprowadzać hasło tak, by nikt inny nie mógł go rozpoznać i zapamiętać
13. W sytuacji gdy zachodzi podejrzenie, że hasło mogła poznać osoba trzecia, nieuprawniona, użytkownik natychmiast ma obowiązek zmienić hasło
14. Administrator Systemu jest odpowiedzialny za czasowe sprawdzanie, blokowanie i usuwanie zbędnych identyfikatorów, nieaktywnych kont za które są odpowiedzialni
15. Administrator powinien dokonywać przeglądu autoryzacji i uprawnień co najmniej raz na 6 miesięcy,
16. Do hasła Administratora Systemu dostęp ma wyłącznie administrator systemu i Administrator Danych.

Proces rozpoczęcia, zakończenia, zawieszenia pracy przez użytkowników

1. Rozpoczęcie pracy odbywa się tylko poprzez wprowadzenie do urządzenia identyfikatora i hasła znanego tylko użytkownikowi
2. Osoby trzecie mogą znajdować się w pomieszczeniu gdzie przetwarzane są dane tylko za zgodą i w towarzystwie osoby uprawnionej do przetwarzania danych
3. Ekrany komputerów należy chronić przed podglądem osób trzecich
4. Monitory komputerów powinny być zaprogramowane na włączenie się wygaszacza po przerwie dłuższej niż 10 minut
5. Podczas puszczania stanowiska pracy każdorazowo użytkownik ma obowiązek wylogować się z systemu.
6. Obowiązuje zakaz robienia kopii całych zbiorów danych – całe zbiory danych mogą być jedynie kopiowane przez Administratora Systemu na potrzeby dokonywania kopii systemu
7. Przesyłanie danych osobowych drogą mailową może odbywać się tylko po ich zaszyfrowaniu
8. Obowiązuje zakaz wynoszenia jakichkolwiek danych osobowych poza obszarach przetwarzania danych na jakichkolwiek nośnikach, nawet w postaci zaszyfrowanej
9. Podczas przetwarzana danych należy jak najczęściej dokonywać zapisu, aby nie utracić tych danych
10. Zakończenie pracy następuje po prawidłowym wylogowaniu się przez użytkowania i wyłączeniu komputera
11. Przed opuszczeniem pokoju należy:
    - Zniszczyć w niszczarce, lub schować do zamykanych na klucz szaf wszelkie wykonane wydruki zawierające dane osobowe
    - Schować do zamykanych na klucz szaf wszelkie teczki z danymi osobowymi
    - Umieścić klucze do szaf w ustalony przeznaczonym do tego miejscu
    - Zamknąć okna
12. Opuszczając pomieszczenie należy zamknąć drzwi na klucz

Tworzenie kopii zapasowych

1. W systemie informatycznym wykorzystującym technologię klient- serwer kopie zapasowe wykonuje się po stronie serwera
2. Nośniki zawierające kopie zapasowe należy odpowiednio oznaczyć „Kopia zapasowa" wraz z podaniem daty sporządzenia.

Częstotliwość wykonywania kopii

1. Kopie zapasowe tworzy się raz w tygodniu dla danych osobowych które uległy zmianie oraz dla aplikacji służących do ich przetwarzania
2. Kopie systemu – wykonuje się raz na 3 miesiące

Przechowywanie kopii

Kopie danych przechowuje Administrator Systemu w zewnętrznej lokalizacji w zamykanym pomieszczeniu wyposażonym w systemy przeciwpożarowe w szafie zamykanej na klucz.

Likwidacja kopii zapasowych

Kopie zapasowe zawierające nieaktualne dane osobowe podlegają fizycznej likwidacji. W przypadku nośników jednorazowych likwidacja polega na fizycznym zniszczeniu w taki sposób, aby niemożliwe było ich odczytanie, nośniki wielokrotnego użytku można ponownie użyć do wykonania na nich kopii zapasowych po uprzednim usunięciu poprzednich danych

Nośniki wielokrotnego użytku nie nadające się do ponownego użytku należy zniszczyć fizycznie np. w niszczarce.

Przechowywanie elektronicznych nośników zawierających dane osobowe

1. Zbiory danych są przechowywane na serwerze Administratora Danych. Dane przetwarzane na poszczególnych komputerach użytkowników są umieszczane każdorazowo w odpowiednich miejscach przydzielonych przez administratora Systemu.
2. Zakazuje się przetwarzania danych na zewnętrznych nośnikach i przesyłania ich pocztą elektroniczną bez szyfrowania.
3. Na nośnikach o których mowa w pkt. 2 dopuszcza się przetwarzanie tylko jednostkowych danych osobowych
4. W przypadku używania nośników od zewnętrznych usługodawców należy wcześniej sprawdzić nośnik za pomocą programu antywirusowego
5. Nośniki informatyczne przechowywane są w zamkniętych szafach i dostęp do nich mają tylko upoważnione osoby
6. Użytkownik komputera przenośnego ma obowiązek ściśle stosować się do postanowień niniejszej instrukcji, oraz dokonywać aktualizacji systemu antywirusowego na żądanie komputera.

Zabezpieczenie systemu przed oprogramowaniem, którego zadaniem jest uzyskanie nieuprawnionego dostępu do danych osobowych

1. Wykrywanie wirusów odbywa się za pomocą oprogramowania zainstalowanego na serwerze i komputerach przez Administratora Systemu,
2. Oprogramowanie antywirusowe pracuje w tle ciągle nadzorując właściwą pracę serwera i komputerów

3. Pomimo ciągłego nadzoru przez oprogramowanie Administrator Systemu ma obowiązek przynajmniej raz w miesiącu dokonać kontroli obecności wirusów w systemie, jak w serwerze i komputerach Gramm
4. Do obowiązku Administratora należy określenie częstotliwości aktualizacji oprogramowania antywirusowego, oraz dokonywanie tej aktualizacji
5. W przypadku pojawienia się informacji o złośliwym oprogramowaniu użytkownik niezwłocznie powiadamia Administratora Systemu
6. Korzystanie z zewnętrznych nośników jest dozwolone tylko i wyłącznie po uprzednim sprawdzeniu ich programem antywirusowym
7. Siec wewnętrzna organizacji chroniona jest zaporami firewall

Przetwarzanie, wprowadzanie, udostępnianie i likwidacja danych osobowych

1. W przypadku zbierania danych osobowych należy poinformować dana osobę o celu i sposobie przechowywania tych danych, oraz o prawie do usunięcia tych danych na jej żądanie – jeżeli nie jest to sprzeczne z wymaganiami prawnymi
2. Zbieranie danych, przetwarzanie, udostępnianie i likwidacja może odbywać się tylko po uzyskaniu indywidualnego upoważnienia od Administratora Danych i tylko w zakresie w jakim upoważnienie pozwala.
3. Na żądanie osoby której dane są przetwarzane należy udzielić jej informacji zgodnie z Rozporządzeniem o RODO, a w przypadku zaistnienia sytuacji utraty danych należy poinformować ją jakie dane zostały utracone i jaki rodzaj działań został podjęty przez organizację w celu minimalizacji skutków tej sytuacji.
4. W przypadku przekazywania urządzeń lub nośników z danymi osobowymi poza obszar ich przetwarzania należy zabezpieczyć je tak aby zapewnić pełną ich rozliczalność, poufność i integralność co oznacza:
5. Stosowanie metod szyfrowania
6. Ograniczenie dostępu do danych za pomocą hasła
7. Stosowanie zabezpieczeń fizycznych i organizacyjnych
8. W przypadku uzyskania danych od osób inne niż te, których dane dotyczą należy odnotować w systemie skąd pochodzą dane
9. W przypadku zgłoszenia przez osobę której dane dotyczą chęci wglądu do danych, chęci dokonania zmiany, bądź chęci usunięcia danych Administrator Danych powinien natychmiast rozpatrzyć taką prośbę i jeżeli nie jest to sprzeczne z prawem i żywotnym interesem Organizacji dane te powinny być usunięte
10. Podczas likwidacji zbiorów danych osobowych należy sporządzić protokół likwidacji danych zawierający informacje dotyczące daty likwidacji danych, przedmiot likwidacji (aplikacja, baza), podpisy osób dokonujących likwidacji.
11. Decyzję o likwidacji danych osobowych może podjąć właściciel danych po uprzednim uzyskaniu zgody Administratora Danych, bądź na prośbę osoby fizycznej które dane dotyczą z uwzględnieniem wymagań z pkt. 3.
12. W przypadku likwidacji elektronicznych nośników danych – należy uprzednio usunąć wszelkie dane osobowe, które się na tym nośniku znajdują.

Postępowanie w przypadku naruszenia bezpieczeństwa systemu informatycznego

- Użytkownik jest zobowiązany natychmiast zawiadomić Administratora Danych, oraz Administratora Systemu jeżeli stwierdzi naruszenie, bądź podejrzenie naruszenia bezpieczeństwa systemu, lub danych osobowych do których ma dostęp, a w szczególności:

- Stwierdzenie naruszenia hasła
- W przypadku stwierdzenia częściowego lub całkowitego braku danych
- Braku dostępu do aplikacji lub serwera
- Wykryciu wirusa w komputerze
- Zauważenia śladów włamania do systemu bądź danych
- Stwierdzenia znacznego spowolnienia systemu
- Stwierdzenia podejrzenia lub stwierdzenia faktycznego stanu kradzieży sprzętu komputerowego, lub dokumentów zawierających dane osobowe
- Stwierdzenia zmiany położenia sprzętu komputerowego
- Zauważenia śladów próby włamania do pomieszczeń z komputerami lub szaf z danymi osobowymi.

W przypadku takich sytuacji należy również rozważyć:

- Natychmiastowe podjęcie działań mających na celu zapobieżenie dalszej utraty danych osobowych
- Rozważyć wstrzymanie dalszej prac bądź jej podjęcia aby nie narazić danych osobowych na zagrożenie
- Zaniechać działań, które mogłyby utrudnić analizę i przeciwdziałanie zaistniałej sytuacji
- Zastosować się do instrukcji i aplikacji jeżeli takie się odwołują do zaistniałej sytuacji
- Nie opuszczać do czasu przybycia Administratora Danych, bądź administratora Systemu pomieszczenia, jeżeli mogłoby to narazić na utratę pozostałych danych osobowych
- Administrator Systemu po otrzymaniu zawiadomienia o utracie bądź podejrzeniu utraty danych niezwłocznie:
- Przeprowadza postępowanie mające na celu wyjaśnienie sytuacji
- Podejmuje działania mające na celu zabezpieczenie pozostałych danych i systemu
- W przypadku stwierdzenia faktycznego naruszenia danych osobowych, bądź ich utraty Administrator Danych dokumentuje w wykazie naruszeń ochrony danych osobowych zaistniałą sytuację
- Administrator Danych podejmuje decyzję o znaczeniu utraty danych i zagrożeniu dla wolności i praw osób, których dane zostały utracone i jeżeli stwierdzi duże zagrożenie w ciągu 72 godzin informuje Organ Nadzorczy.
- Jednocześnie Administrator Danych jeżeli jest to konieczne informuje osoby, których dane zostały utracone o znaczeniu tej utraty i działaniach podjętych przez organizację mających na celu zminimalizowanie skutków tej utraty,
- Administrator Danych i Administrator Systemu podejmują odpowiednie działania mające na celu zapobieżenie ponownej utraty danych
- Administrator Systemu ma obowiązek zgłaszać Administratorowi Danych każdorazowe nieautoryzowane użycie nośników i programów przez użytkowników systemu
- Administrator Systemu raz w roku składa Administratorowi Danych kompleksowy raport z analizą zarządzania systemem danych.

Postanowienia końcowe

- W sprawach nieokreślonych w tej instrukcji należy stosować instrukcje obsługi i zalecenia producentów urządzeń i programowania

- Każda osoba upoważniona do przetwarzania danych jest zapoznawana z tą instrukcją
- Niestosowanie się do tej instrukcji przez pracowników upoważnionych do przetwarzania danych może narazić organizację na straty wizerunkowe, oraz straty finansowe oraz traktowane będzie jako poważne naruszenie obowiązków pracowniczych i może skutkować rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu Pracy.
- Niniejsza instrukcja wchodzi w życie z dniem

Załącznik nr 7 – Instrukcja ocena ryzyka przetwarzania danych

1. CEL INSTRUKCJI

Celem niniejszej instrukcji jest określenie działań koniecznych do spełnienia wymagań Rozporządzenia 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) dotyczących oceny i zarządzania ryzykiem w procesie przetwarzania danych oraz zapewnienie odpowiedzi na poniżesz pytania:

- Kto bierze udział w procesie oceny ryzyka dla zarządzania danych i jak ten proces jest zorganizowany?
- W jaki sposób dokonuje się oceny ryzyka?
- Jakie są zagrożenia i jaka jest możliwość wystąpienia?
- Kiedy należy podjąć działania w wyniku oceny ryzyka

2. PRZEDMIOT INSTRUKCJI

Przedmiotem instrukcji jest określenie znaczenia zagrożeń mogących wystąpić w organizacji dotyczących w szczególności zasad przetwarzania i nadzoru nad powierzonymi danymi osobowymi, oceny możliwości ich wystąpienia oraz określenia znaczenia tych ryzyk dla operacji przetwarzania danych osobowych, ze szczególnym uwzględnieniem ryzyka dla osób, których dane są przetwarzane. Instrukcja opisuje sposób oceny i postępowania z zagrożeniami określonymi w Polityce Bezpieczeństwa Przetwarzania Danych Osobowych, zidentyfikowanymi w poszczególnych procesach przetwarzania, oraz z zagrożeniami, które nie zostały jeszcze rozpoznane, a zostaną zidentyfikowane w trakcie dalszego funkcjonowania organizacji.

3. ZAKRES ZASTOSOWANIA

Instrukcja obowiązuje w Gramm Technika Sp. z.o.o . i ma zastosowanie w stosunku do:
- oceny ryzyka dla procesu przetwarzania danych w organizacji ,
- oceny ryzyka związanego z niespełnieniem wymagań prawnych,
- oceny możliwości wystąpienia ryzyka określonego w poszczególnych procesach przetwarzania danych osobowych w organizacji

4. DEFINICJE

Na potrzeby instrukcji i działań organizacji zastosowano następujące definicje:

- **Ryzyko** — zagrożenie, prawdopodobieństwo wystąpienia zdarzeń (pozytywnych i negatywnych), które mogą mieć wpływ na organizację, jej zdolność do spełnienia wymagań prawny, właściwego nadzoru nad powierzonymi danymi osobowymi, osiągnięcia zamierzonych celów organizacji, lub powodują odchylenia od oczekiwanych stanów. Istnieją dwa źródła ryzyka: zagrożenia bezpośrednie (zdarzenia szkodliwe), które powoduj że cele nie zostaną osiągnięte, - szanse (zdarzenia korzystne), które przy właściwych działaniach dają możliwość skutecznego osiągnięcia celów.

- **Czynnik ryzyka** - okoliczności, stan prawny, stan faktyczny, działania, zaniechanie działań i wydarzenia zewnętrzne oraz wewnętrzne, które mogą ale nie muszą wywołać ryzyko wystąpienia nieprawidłowości. To przyczyny wystąpienia ryzyka /zagrożenia.
- **Analiza ryzyka** — metoda oceny podatności procesu, systemu lub grupy systemów na czynniki ryzyka. Jej celem jest wskazanie tych obszarów gdzie ryzyko jest największe, oraz gdzie Organizacja powinna podjąć działania.
- **zespół interdyscyplinarny** – zespół powołany przez Prezesa organizacji do rozpatrzenia, oceny zagrożeń, zespół składa się z: Administratora Danych, Administratora Systemu, oraz przedstawicieli osób odpowiedzialnych za zarządzanie danymi z każdego zbioru danych
- **prawdopodobieństwo wystąpienia ryzyka** – możliwość zmaterializowania się danego zagrożenia oceniona liczbowo ***1 – 5*** – skala zawiera również opis dla poszczególnych wartości.
- **skutki wystąpienia ryzyka** – opis za pomocą kategorii, klasyfikacji i charakterystyki skutków zmaterializowania się danego zagrożenia dla trzech podstawowych charakterystyk: ***biznesu, infrastruktury, osoby - osób których dane są przetwarzane.***
- **przeniesienie ryzyka** – sposób postępowania z ryzykiem np. przeniesienie na inną instytucję, np. poprzez ubezpieczenie.
- **tolerowanie ryzyka** – w przypadku, gdy istnieją określone trudności w przeciwdziałaniu ryzykom, a także, gdy koszty podjętych działań mogą przekroczyć przewidywane korzyści.
- **przeciwdziałanie** – działania pozwalające na ograniczenie ryzyka do akceptowalnego poziomu, dzięki wzmocnieniu mechanizmów kontroli zarządczej (poprzez procedury, wytyczne, zasady, nadzór, itd.) wbudowane w realizowane procesy.
- **przesunięcie w czasie** (wycofanie się) – zawieszenie działań rodzących zbyt duże ryzyko.

5. ODPOWIEDZIALNOŚCI

Odpowiedzialności wynikające z zastosowania instrukcji są następujące:

- **Właściciel procesu oceny ryzyka dla procesu przetwarzania danych** – osoba w organizacji, która wyznacza zespół interdyscyplinarny do rozpatrzenia i oceny znanych zagrożeń, oraz podejmuje końcową decyzję dotyczącą słuszności wyników oceny, a także podejmuje decyzje dotyczącą wdrożenia określonych działań – w przypadku Gramm Technika Sp. z o.o. – jest to Administrator Danych – V-ce Prezes organizacji.

- **Właściciele procesów przetwarzania danych** – osoby upoważnione na podstawie Indywidualnego upoważnienia do przetwarzanie danych - odpowiedzialne za przekazanie informacji do Administratora Danych, Administratora Systemu, w przypadku zidentyfikowania zagrożenia w ich procesach przetwarzania danych, bądź zmaterializowania się ryzyk wcześniej zidentyfikowanych.

- **Zespół interdyscyplinarny –** odpowiedzialny jest za zidentyfikowanie na podstawie znanych faktów zagrożeń, które mogą dotyczyć procesów przetwarzania danych w organizacji, określenie jaki wpływ na organizację i jej system i procesy przetwarzania danych może mieć zmaterializowanie

się danego zagrożenia, określenie czy są wymagane dodatkowe działania w celu zmniejszenia skutków materializacji danego zagrożenia przy użyciu wymienionych w instrukcji działań.

6. SPOSÓB POSTĘPOWANIA

6.1. Powołanie zespołu interdyscyplinarnego:

Osoba odpowiedzialna za proces oceny ryzyka – w Gramm Technika V-ce Prezes organizacji – powołuje zespół interdyscyplinarny, którego zadaniem jest zebranie się, zidentyfikowanie i ocena znanych ryzyk związanych z funkcjonowaniem Systemu przetwarzania danych w organizacji w przestrzeni biznesowej, a także ryzyk w zidentyfikowanych procesach w organizacji. Oceniane ryzyka dotyczą przede wszystkich możliwych negatywnych skutków dla osób, których dane w organizacji są przetwarzane oraz wymagań prawnych. Zespół interdyscyplinarny po określeniu ryzyk poddaje je ocenie i opiniuje do V-ce Prezesa dla których zdefiniowanych ryzyk należy podjąć dodatkowe działania. Prezes podejmuje końcowe decyzje, czy zaopiniowane działania są potrzebne i czy należy je wdrożyć w życie, a także podejmuje decyzje kiedy ewentualnie działania te zostaną wdrożone.

6.2. Analiza ryzyka.

Powołany zespół interdyscyplinarny w oparciu o fakty, dane dotyczące funkcjonowania organizacji, dane dotyczące Sytemu informatycznego i jego zabezpieczeń, znajomość charakteru organizacji, znajomość wymagań prawnych dotyczących działania organizacji, znajomość procesów przetarzania danych w organizacji, znajomość własnych potrzeb, w oparciu o dokumentacje – Politykę Bezpieczeństwa Przetwarzania Danych, Instrukcję Zarządzania Systemem Informatycznym oraz dokumenty związane – definiuje ryzyka jakie mogą dotyczyć zagrożeń dla procesu przetwarzania danych osobowych w organizacji oraz korzystając z poniższych narzędzi dokonuje analizy tych ryzyk.

- **PRAWDOPODOBIEŃSTWO WYSTĄPIENIA RYZYKA**

Zdefiniowane ryzyka oceniane są przez pryzmat prawdopodobieństwa wystąpienia według poniższego schematu:

Skala ryzyka	prawdopodobieństwo wystąpienia - zmaterializowania	Opis
1	**Bardzo rzadkie**	Może wystąpić tylko wyjątkowych okolicznościach. Może wystąpić raz na 50 lub więcej lat.
2	**Rzadkie**	Nie oczekuje się, że się może zdarzyć i/lub nie jest w ogóle udokumentowane w organizacji i/lub zdarzenia nie wystąpiły w organizacji , urządzeniach, i/lub istnieje mała szansa, powód, czy też inne okoliczności aby zdarzenia mogły wystąpić. Mogą one wystąpić raz na 20 lat.
3	**Możliwe**	Może zdarzyć się w określonym czasie w połączeniu z innymi określonymi okolicznościami i/lub występuje rzadko jako przypadkowe zdarzenie i/lub może być znane jako udokumentowane zdarzenie lub cząstkowo przekazywane w formie ustnej i/lub bardzo mało znanych zdarzeń i/lub jest pewna szansa, powód, czy też urządzenia powodujące, że zdarzenie może wystąpić. Może zdarzyć się raz na 5 lat
4	**Prawdopodobne**	Jest prawdopodobne, że wystąpi w większości okolicznościach i/lub ryzyko to materializowało są systematycznie i jest udokumentowane i/lub występuje znaczna szansa, powód, lub urządzenia pozwalające na jego wystąpienie.

		Może zdarzyć się raz na 6 miesięcy
5	**Bardzo prawdopodobne**	Oczekuje się, że zdarzy się w większości okoliczności i/lub ryzyko to jest bardzo dobrze udokumentowane i/lub znane jest pracownikom. Może wystąpić raz w miesiącu

- **MOŻLIWE SKUTKI WYSTĄPIENIA RYZYKA**

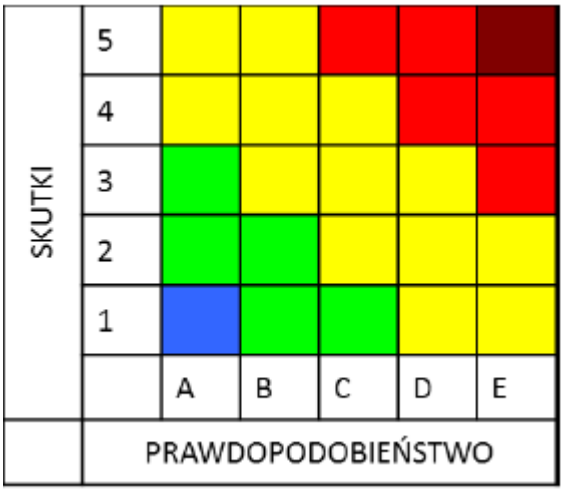
Zdefiniowane ryzyka oceniane są przez pryzmat możliwych skutków wystąpienia danego zagrożenia według poniższych:

Skala	Skutki	Kategoria	Opis (B – biznes , I – infrastruktura , S – środowisko)
A	**Nieistotne**	**Biznes**	Nie ma znaczenia dla powiązań biznesowych. Nikt lub mała liczba osób została zaangażowana w rozwiązanie problemu, zminimalizowanie ryzyka, brak kosztów biznesowych.
		Infrastruktura	Brak wpływu lub bardzo niewielki na urządzenia i system informatyczny. Brak lub niewielkie straty finansowe do 100 Euro,
		Osoba, której dane osobowe są przetwarzane	Brak zagrożenia dla osoby, osób, których dane są przetwarzane
B	**Małe**	**Biznes**	Niewielkie znaczenie dla biznesu, drobne niedogodności. Wymagane zaangażowanie Kierownictwa średniego szczebla w rozwiązanie problemu zaistniałego ryzyka. Możliwe niewielkie straty wizerunkowe, możliwe niewielkie koszty finansowe biznesu do 300 Euro,
		Infrastruktura	Występują niewielkie uszkodzenia w Infrastrukturze, jednakże nie związane z uszkodzeniami systemu informatycznego. Niewielkie straty finansowe. Nie wymagane większe nakłady finansowe na infrastrukturę w przedziale od 200 do 400 Euro. Brak wpływu na funkcjonowanie procesu przetwarzania, przepływu danych osobowych
		Osoba, której dane osobowe są przetwarzane	Niewielki wpływ na przetwarzane dane osób, osoby, brak zagrożenia dla tych osób
C	**Średnie**	**Biznes**	Duże znaczenie wizerunkowe, konieczne zaangażowanie Najwyższego Kierownictwa w rozwiązanie problemu, koniecznie poniesienie kosztów biznesowych w przedziale od 300 do 500 Euro,
		Infrastruktura	Wymagane wyłączenie systemu informatycznego do 7 dni, Występują odczuwalne utrudnienia w funkcjonowaniu organizacji. Występują niewielkie zakłócenia w zarządzaniu danymi, konieczne zaangażowanie Administratora Danych i Administratora Systemu konieczne poniesienie kosztów naprawy infrastruktury informatycznej w przedziale od 400 do 2500 Euro.
		Osoba, której dane osobowe są przetwarzane	Utrata pewnych danych osobowych, lecz nie mająca wpływu na bezpieczeństwo finansowe i bezpieczeństwo fizyczne osób, których dane finansowe są przetwarzane – np. nieodwracalna utrata części danych poprzez uszkodzenie serwera – konieczne pozyskanie danych po raz kolejny
D	**Duże**	**Biznes**	Duże straty wizerunkowe, Konieczne uruchomienie ubezpieczeń i zaangażowanie Administratora Danych i Administratora Systemu w rozwiązanie problemów, Możliwa konieczność złożenia zgłoszenia i wyjaśnień do Organu Nadzorczego Oczekiwane dodatkowe kontrole urzędów państwowych, możliwe kary finansowe.
		Infrastruktura	Istotne uszkodzenie urządzeń przetwarzających dane, bądź ich utrata, bądź inne istotne uszkodzenie infrastruktury, oraz utrata części powierzonych danych osobowych, konieczne poniesienie znacznych kosztów w rozwiązanie problemu, konieczne poniesienie znacznych kosztów naprawy infrastruktury w przedziale powyżej 2500 Euro.

		Osoba, której dane osobowe są przetwarzane	Utrata części powierzonych danych osobowych, możliwe sytuacje nękania osób których dane zostały utracone przez osoby trzecie, możliwa konieczność poniesienia strat finansowych przez osoby których dane zostały utracone, możliwe zagrożenie dla finansów i kont bankowych osób których dane zostały utracone
E	**Katastrofalne**	**Biznes**	Duże straty wizerunkowe, utrata zaufania urzędów państwowych, Konieczność zgłoszenia do Organu Nadzorczego uruchomienia ubezpieczeń, straty biznesowe w przedziale powyżej 100000 Euro, możliwe zamknięcie organizacji. Pewne dodatkowe kontrole urzędów państwowych i kary finansowe.
		Infrastruktura	Rozległe zniszczenia infrastruktury bądź systemu informatycznego. Niemożność funkcjonowania przez okres powyżej 30 dni, utrata większości danych, które organizacja przetwarzała brak opłacalności reperacji istniejącej infrastruktury.
		Środowisko	Całkowita utrata powierzonych organizacji danych osobowych na rzecz osób trzecich, których zamiarem jest zaszkodzenie osobom fizycznym poprzez kradzież tożsamości, realne zagrożenie utraty finansów, zdrowia, lub życia osób których dane zostały utracone.

Poniżej tabela zestawienia zależności pomiędzy skutkami wystąpienia ryzyka i prawdopodobieństwem jego wystąpienia, oraz za pomocą kolorów określone kategorie danych ryzyk w przypadku określonych zależności. Po przenalizowaniu ryzyk uznanych przez zespół interdyscyplinarny za istotne należy przedstawić dla tych ryzyk ocenę wynikającą z zastosowania poniższej tabeli.

Tabela do analizy ryzyka z korelacją:



Wartości i znaczenie ryzyka oznaczono kolorami:

- minimalne (kolor niebieski) - **A**
- małe (kolor zielony) - **T**
- średnie (kolor żółty) - **WT**
- duże (kolor czerwony) - **N**
- ekstremalne (kolor brunatny) - **N**

Kolejnym elementem jest określenie kryteriów akceptacji ryzyka w ramach 4 kategorii wyrażonych kolorami. Organizacja przyjęła następujące kryteria akceptacji ryzyk:

- ryzyko minimalne – akceptowalne (**A**) - nie wymagane są żadne dodatkowe środki bezpieczeństwa, akceptowane są aktualne rozwiązania i przypisane im siły i środki, działania monitorujące. W tabeli do analizy kolor **niebieski**
- ryzyko tolerowane (dopuszczalne) (**T**) - należy dokonać oceny alternatyw czy wprowadzenie niewielkich zmian organizacyjnych, funkcjonalnych oraz technicznych nie przyczyni się do poprawy funkcjonowania organizacji i zmniejszenia ewentualnych skutków zagrożenia. W tabeli do analizy kolor **zielony**
- ryzyko warunkowo tolerowane (**WT**) - należy wprowadzić dodatkowe działania i środki bezpieczeństwa w terminie max. 1 miesiąca, należy ulepszyć stosowane rozwiązania. W tabeli do analizy **żółty**

- ryzyko nieakceptowane (N) - należy podjąć natychmiastowe działania w celu zwiększenia bezpieczeństwa, wprowadzić dodatkowe/ nowe rozwiązania. W tabeli do analizy kolor **czerwony** i **brunatny**

Po przedstawieniu przez zespół interdyscyplinarny oceny ryzyka Prezes podejmie decyzje, które ryzyka należy w pierwszej kolejności ograniczyć poprzez zastosowanie działań natychmiastowy.