ATHENA

Członek Grupy GrECo

Polityka bezpieczeństwa przetwarzania danych osobowych w Athena Spółka z o.o.

Wersja 1.0

01.01.2022

Spis treści:

1.1 Wstęp

Realizując konstytucyjne prawo każdej osoby do ochrony życia prywatnego oraz postanowienia rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) w celu zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ww. rozporządzenia oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, wprowadza się następującą politykę bezpieczeństwa danych.

1.2 Przedmiot regulacji

1. Polityka bezpieczeństwa przetwarzania danych osobowych w Athena Spółka z ograniczoną odpowiedzialnością (zwana dalej „Polityką bezpieczeństwa") określa:
   1) wytyczenie podstawowych zasad i wymagań bezpieczeństwa systemów teleinformatycznych, w których są wytwarzane, przetwarzane, przekazywane i przechowywane zasoby informacji,
   2) role i obowiązki związane z utrzymaniem bezpieczeństwa danych osobowych w Spółce.
2. Postanowienia Polityki bezpieczeństwa odnoszą się do całości systemów informatycznych Spółki, rozpatrywanych w kontekście infrastruktury technicznej Spółki, jego organizacji oraz posiadanej kadry.
3. Przedstawione w niniejszym dokumencie środki i metody ochrony informacji dotyczą wszelkich jej form zapisu, w tym informacji zapisanej na nośnikach elektronicznych, optycznych, magnetycznych i papierowych.
4. Przedstawione w niniejszym dokumencie metody ochrony danych osobowych dotyczą lokalizacji Spółki w Poznaniu.
5. Za wprowadzenie Polityki bezpieczeństwa odpowiada Zarząd Spółki.
6. Zarząd Spółki, w uzasadnionych i szczególnych przypadkach może zlecać pewne zadania w zakresie realizacji Polityki bezpieczeństwa podmiotom zewnętrznym po podpisaniu umowy o zachowaniu poufności.

1.3 Definicje

Ilekroć w dokumencie jest mowa o:

1) **rozporządzeniu** – rozumie się przez to rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
2) **danych osobowych** – rozumie się przez to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora, takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
3) **zbiorze danych** – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
4) **przetwarzaniu danych** – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub

modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

5) **systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
6) **zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
7) **usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
8) **administratorze danych** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;
9) **zgodzie osoby, której dane dotyczą** – oznacza to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
10) **odbiorcy danych** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
11) **państwie trzecim** – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego;
12) **środkach technicznych i organizacyjnych** – należy przez to rozumieć środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych;
13) **ograniczeniu przetwarzania** – należy przez to rozumieć oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
14) **profilowaniu** – oznacza to dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
15) **pseudonimizacji** – oznacza to przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
16) **podmiocie przetwarzającym** – oznacza to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
17) **naruszeniu ochrony danych osobowych** – oznacza to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

1.4 Zgodność

1. Polityka bezpieczeństwa oraz wynikające z niej szczegółowe regulacje muszą być zgodne z powszechnie obowiązującym prawem, w szczególności z:
   1) rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
   2) ustawą o ochronie danych osobowych z dnia 24 maja 2018 r.
   3) ustawą o pośrednictwie ubezpieczeniowym z dnia 22 maja 2003 r.
2. Każda umowa zewnętrzna zawarta przez Spółkę musi być zgodna z Polityką bezpieczeństwa.

1.5 Zakres

1. Politykę bezpieczeństwa stosuje się do:
   1) danych osobowych Klientów, Dostawców i Kontrahentów przetwarzanych w systemie informatycznym i w formie papierowej,
   2) wszystkich informacji dotyczących danych pracowników Spółki,
   3) wszystkich danych kandydatów do pracy zbieranych na etapie rekrutacji,
   4) informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
   5) rejestru osób dopuszczonych do przetwarzania danych osobowych,
   6) innych dokumentów zawierających dane osobowe.
2. Zakresy określone przez dokumenty Polityki bezpieczeństwa mają zastosowanie do całego systemu informatycznego Spółki, a w szczególności do:
   1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych, w których przetwarzane są dane osobowe podlegające ochronie,
   2) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane dane osobowe podlegające ochronie,
   3) wszystkich pracowników Spółki, konsultantów, stażystów i innych osób mających dostęp do danych osobowych podlegających ochronie.
3. Do stosowania zasad określonych przez dokumenty Polityki bezpieczeństwa zobowiązani są wszyscy pracownicy Spółki, konsultanci, stażyści oraz inne osoby mające dostęp do danych osobowych podlegających ochronie.

1.6 Przetwarzanie danych osobowych

1. Systemy informatyczne, służące do przetwarzania danych osobowych, muszą spełniać wymogi obowiązujących aktów prawnych regulujących zasady gromadzenia i przetwarzania danych osobowych.
2. Do tworzenia kopii bezpieczeństwa danych osobowych w postaci elektronicznej służą indywidualne systemy archiwizowania dla poszczególnych systemów przetwarzania.
3. Kopie bezpieczeństwa oraz dokumenty papierowe zawierające dane osobowe przechowuje się w warunkach uniemożliwiających dostęp do nich osobom nieuprawnionym.

1.7 Administrator Danych

1. Administrator danych w szczególności:
   a) uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.
   b) prowadzi Rejestr czynności przetwarzania.
   c) prowadzi Rejestr żądań dotyczących ochrony danych.
   d) prowadzi Rejestr naruszeń ochrony danych osobowych.
2. Na podstawie art. 37 Rozporządzenia w Spółce nie powołuje się Inspektora Ochrony Danych.

1.8 Opis ryzyk i zagrożeń

1. W Spółce zidentyfikowano możliwe zagrożenia wewnętrzne i zewnętrzne, spowodowane przez następujące działania:

   a) zagrożenia zewnętrzne: sabotaż, szpiegostwo przemysłowe, działania terrorystyczne.
   b) zagrożenia wewnętrzne: awarie/zniszczenie sprzętu, niewłaściwe użycie sprzętu elektronicznego, błędy pracowników, przestępstwo pracownika, niezgodne z procedurami użycie smartfonów.

2. Na podstawie analizy czynników zagrożeń i statystyki dotychczasowych incydentów Spółka ocenia podatność na zagrożenia jako niską (w ostatnich latach nie wystąpiły żadne incydenty grożące prawom wolności osób, których dane dotyczą).

1.9 Środki techniczne i organizacyjne

1. Zgodnie z umową o powierzenie przetwarzania danych osobowych, zawartą w dniu 2 sierpnia 2021 roku z GrECo International Holding AG, wszystkie dane wykorzystywane bezpośrednio w procesie przetwarzania danych osobowych przechowywane są na serwerach w Austrii w siedzibie spółki GrECo International AG przy Elmargasse 2-4, A-1191 Wiedeń, Austria. Znajdujące się na stałe w siedzibie Spółki komputery są jedynie urządzeniami dostępowymi pozbawionymi możliwości przechowywania plików w trybie offline – dostęp do zasobów serwera odbywa się z wykorzystaniem wirtualnego pulpitu.

2. Część danych (z wyłączeniem danych osobowych) znajduje się w folderach offline zmapowanych dysków sieciowych na przestrzeni dyskowej komputerów przenośnych wykorzystywanych przez pracowników Spółki i jest chroniona przed nieautoryzowanym dostępem zabezpieczeniami dostarczanymi przez producenta sprzętu oraz oprogramowania.

3. Wszystkie kopie zapasowe niezależnie od rodzaju nośnika znajdują się w siedzibie GrECo International Holding AG przy Elmargasse 2-4, A-1191 Wiedeń, Austria. Taśmy z comiesięcznymi kopiami bezpieczeństwa są przechowywane w specjalnie do takich taśm przeznaczonym, ogniotrwałym sejfie poza siedzibą Spółki macierzystej.

4. W celu ochrony danych spełniono wymogi, o których mowa w rozporządzeniu, w szczególności:
   a) przeprowadzono analizę ryzyka w stosunku do zasobów biorących udział w poszczególnych procesach,
   b) do przetwarzania danych zostały dopuszczone wyłącznie osoby upoważnione przez administratora danych;
   c) zawarto umowy powierzenia przetwarzania danych osobowych
   d) została opracowana i wdrożona niniejsza polityka bezpieczeństwa.

5. Środki techniczne i organizacyjne są opisane w Załączniku nr 10.

6. Zbiory danych osobowych przechowywane są w pomieszczeniach zabezpieczonych drzwiami zwykłymi (niewzmacnianymi, nieprzeciwpożarowymi).
7. Dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych, objęty jest systemem kontroli dostępu.
8. Dostęp do wszystkich pomieszczeń, w tym również tych w których przetwarzane są zbiory danych osobowych, kontrolowany jest przez całodobowy system monitoringu elektronicznego, prowadzonego przez Agencję Ochrony Joker sp. z o.o.
9. Zbiory danych osobowych w formie papierowej przechowywane są w zamkniętych niemetalowych szafach.
10. Zbiory danych osobowych pracowników w formie papierowej przechowywane są w zamykanej szafie stalowej oraz w biurze firmy Haxo sp. z o.o. świadczy usługi kadrowo-płacowe dla Athena sp. z o.o.
11. Pomieszczenia, w których przetwarzane są zbiory danych osobowych, zabezpieczone są przed skutkami pożaru za pomocą wolnostojących gaśnic.
12. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone przez profesjonalną firmę zewnętrzną.
13. W celu ochrony danych osobowych stosuje się następujące środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej:
    a) komputery służące do przetwarzania danych osobowych nie są połączone z lokalną siecią komputerową;
    b) zastosowano urządzenia typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania;
    c) dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
    d) zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych;
    e) zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł;
    f) zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych;
    g) zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej;
    h) zastosowano środki ochrony przed szkodliwym oprogramowaniem, takim jak np. robaki, wirusy, konie trojańskie, rootkity;
    i) użyto system Firewall do ochrony dostępu do sieci komputerowej;
    j) użyto system IDS/IPS do ochrony dostępu do sieci komputerowej.
14. W celu ochrony danych osobowych stosuje się następujące środki ochrony w ramach narzędzi programowych i baz danych:
    a) wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych;
    b) zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych;
    c) dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
    d) zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego;
    e) zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.
15. W celu ochrony danych osobowych stosuje się następujące środki organizacyjne:
    a) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych;
    b) przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego;

c) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
d) w umowach o pracę i w umowach ze zleceniobiorcami stosuje się klauzule o zachowaniu poufności.
e) osoby z zewnątrz dopuszczone do informacji chronionych w Spółce, podpisują zobowiązanie dotyczące zachowania poufności w trybie art. 266 § 1 Kodeksu karnego.

1.10 Dostęp osób trzecich

1. Dostęp osób trzecich do aktywów systemu informatycznego, takich jak usługodawcy lub partnerzy, musi być uzasadniony i odbywać się na ściśle określonych zasadach zatwierdzonych przez ADO.
2. Dostęp partnerów czy firm zewnętrznych, realizujących kontrakty związane z koniecznością dostępu do infrastruktury teleinformatycznej musi odbywać się na szczególnych zasadach, określonych w zawieranych obowiązkowo umowach.
3. Udostępnianie danych osobowych podmiotom upoważnionym do ich otrzymania na podstawie przepisów prawa powinno odbywać się wg określonych odrębnymi przepisami procedur postępowania.

1.11 Procedura współpracy z podmiotami zewnętrznymi

1. Każdorazowe skorzystanie z usług podmiotu przetwarzającego jest poprzedzone zawarciem umowy powierzenia przetwarzania danych osobowych.
2. Nie rzadziej niż raz w roku oraz każdorazowo przed zawarciem umowy powierzenia przetwarzania danych osobowych administrator danych weryfikuje zgodność z rozporządzeniem wszystkich podmiotów przetwarzających, z których usług korzysta lub ma zamiar skorzystać z wykorzystaniem listy kontrolnej.
3. Niepotrzebne w bieżącej działalności dokumenty zawierające dane osobowe są brakowane lub archiwizowane za pośrednictwem zewnętrznej firmy wyspecjalizowanej w tego typu usługach. Odpowiedzialność za prawidłową archiwizację i brakowanie oraz metody ich przeprowadzania reguluje umowa między Spółką a każdorazowym Usługodawcą.

1.12 Procedura udzielenia informacji na żądanie

1. Administrator danych rozpatruje indywidualnie każdy przypadek zgłoszenia woli skorzystania z praw przewidzianych w rozporządzeniu przez osobę, której dane dotyczą.
2. Administrator danych niezwłocznie realizuje następujące prawa osób, których dane dotyczą:
   a) prawo dostępu do danych,
   b) prawo do sprostowania danych,
   c) prawo do usunięcia danych,
   d) prawo do przenoszenia danych,
   e) prawo do sprzeciwu wobec przetwarzania danych,
   f) prawo do niepodlegania decyzjom oparty wyłącznie na profilowaniu.
3. W przypadku realizacji prawa do sprostowania, usunięcia i ograniczenia przetwarzania danych administrator danych niezwłocznie informuje odbiorców danych, którym udostępnił on przedmiotowe dane, chyba że jest to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.
4. Administrator danych odmawia realizacji praw osób, których dane dotyczą, jeżeli możliwość taka wynika z przepisów rozporządzenia, jednak każda odmowa realizacji praw osób, których dane dotyczą, wymaga uzasadnienia z podaniem podstawy prawnej wynikającej z rozporządzenia.
5. Procedura udzielenia informacji na żądanie została opisana w Załączniku nr 3.

6. Wzór pisma „Udzielenie informacji zgodnie z art. 15 RODO" znajduje się w Załączniku nr 4.
7. Wzór Rejestru żądań dotyczących realizacji praw osób znajduje się w Załączniku nr 5.

1.13 Procedura odbierania zgód oraz informowania osób

1. W każdym przypadku pobierania danych bezpośrednio od osoby, której dane dotyczą, administrator danych informuje osobę, której dane dotyczą o przysługujących jej prawach.
2. W każdym przypadku odbierania zgody od osoby, której dane dotyczą, korzysta się z klauzul zgody zgodnie z załącznikami nr 10 i 11.

1.14 Procedura usunięcia danych na żądanie

1. Administrator danych rozpatruje indywidualnie każdy przypadek żądania usunięcia danych, zgłoszonego przez osobę, której dane dotyczą.
2. Administrator sprawdza, czy dane są przechowywane w systemach i zasobach archiwalnych i jeżeli jest to możliwe, bez zbędnej zwłoki zleca usunięcie danych.
3. Procedura usuwania danych na żądanie została opisana w Załączniku nr 6.

1.15 Procedura zarządzania naruszeniami ochrony danych

1. W przypadku naruszenia ochrony danych każdy pracownik administratora ma obowiązek:
   a) niezwłocznie zawiadomić administratora o stwierdzonym naruszeniu lub podejrzeniu wystąpienia faktu naruszenia,
   b) podjęcia czynności niezbędnych do powstrzymania skutków naruszenia
   c) zabezpieczenia dowodów umożliwiających ustalenie przyczyny oraz skutki naruszenia
   d) zaniechania działań mogących utrudnić analizę wystąpienia naruszenia.
2. W każdym przypadku naruszenia ochrony danych osobowych administrator danych weryfikuje, czy naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
3. Administrator danych w przypadku stwierdzenia, że naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, zawiadamia niezwłocznie organ nadzorczy, jednak nie później niż w ciągu 72 godz. od identyfikacji naruszenia.
4. Administrator danych zawiadamia osoby, których dane dotyczą, w przypadku wystąpienia wobec nich naruszeń skutkujących ryzykiem naruszenia ich praw lub wolności, chyba że zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka wystąpienia ww. naruszenia.
5. Administrator danych dokumentuje naruszenia, które skutkują naruszeniem praw i wolności osób fizycznych w Rejestrze, którego wzór stanowi Załącznik nr 8.
6. Procedura zgłoszenia naruszeń ochrony danych została opisana w Załączniku nr 7.
7. Wzór zgłoszenia naruszenia organowi nadzoru jest dostępny na stronie www.uodo.gov.pl.

1.16 Konsekwencje naruszenia Polityki bezpieczeństwa

W przypadku naruszenia przez pracownika Spółki przepisów Polityki bezpieczeństwa, przewiduje się możliwość:

a) pociągnięcia pracownika do odpowiedzialności materialnej na zasadach określonych w przepisach prawa pracy,

b) pociągnięcia pracownika do odpowiedzialności dyscyplinarnej, ze zwolnieniem dyscyplinarnym włącznie, na zasadach określonych w przepisach prawa pracy,
c) powiadomienia właściwych organów o podejrzeniu popełnienia przestępstwa lub wytoczenia powództwa cywilnego.

1.17 Zarządzanie aktywami systemów informatycznych

Zarządzanie aktywami systemów informatycznych, w szczególności systemów MIS, PIMS i WebBase, zostało opisane w poszczególnych Rejestrach czynności przetwarzania.

1.18 Dokumenty powiązane

Załączniki do Polityki bezpieczeństwa:

1. Załącznik nr 1 – Wykaz zbiorów danych
2. Załącznik nr 2 – Rejestry czynności przetwarzania:
    - Rejestr dotyczący systemu MIS
    - Rejestr dotyczący systemu PIMS
    - Rejestr pionu Księgowości i Administracji (F&A)
    - Rejestr Pionu Revenue Management (RM)
    - Rejestr Pionu HR (Zarządzanie personelem)
    - Rejestr dotyczący poczty elektronicznej
    - Rejestr dotyczący bazy spotkań
    - Rejestr dotyczący współpracy z Dostawcami
    - Rejestr dotyczący pośrednictwa ubezpieczeniowego (S&AM / RIT)
    - Rejestr dotyczący marketingu.
3. Załącznik nr 3 – Procedura udzielenia informacji na żądanie.
4. Załącznik nr 4 – Wzór pisma: Udzielenie informacji zgodnie z art. 15 RODO
5. Załącznik nr 5 – Rejestr żądań dotyczących ochrony danych.
6. Załącznik nr 6 – Procedura usunięcia danych na żądanie.
7. Załącznik nr 7 – Procedura zarządzania naruszeniami ochrony danych osobowych.
8. Załącznik nr 8 – Rejestr naruszeń ochrony danych osobowych.
9. Załącznik nr 9 – Procedura przetwarzania danych osobowych
10. Załącznik nr 10 – Środki bezpieczeństwa (organizacyjne i techniczne) ochrony danych.
11. Załącznik nr 11 – Wzór zgody na przetwarzanie danych osobowych dotyczących zdrowia.
12. Załącznik nr 12 – Wzór zgody na przetwarzanie danych biometrycznych.
13. Załącznik nr 13 – Polityka prywatności.

Załącznik nr 1 – Wykaz zbiorów danych osobowych i programów do przetwarzania tych danych

Nr	Nazwa zbioru danych	Opis zbioru danych	System informatyczny do przetwarzania zbioru danych
1.	Dane Klientów (ubezpieczających i ubezpieczonych)	Baza danych zawartych umów ubezpieczenia, związanych z nimi szkód, płatności, rozliczeń i wszystkich innych informacji, które są potrzebne do zarządzania portfelem umów ubezpieczenia. **Są to następujące dane osobowe**: Imię i nazwisko, Adres, Nr telefonu, Telefon komórkowy, Nr faksu, Adres e-mail, Strona www, Płeć, Stan cywilny, Nazwisko rodowe, Obywatelstwo, Konto bankowe - IBAN / SWIFT, Rodzaj ubezpieczenia (linia ubezpieczenia), Nr polisy, Początek okresu ubezpieczenia, Koniec okresu ubezpieczenia, Opis ryzyka, Zakres ochrony ubezpieczeniowej, Kwota ubezpieczenia, Dane dotyczące składek (stawka), Data płatności składek, Dane dotyczące cesji bankowych umowy ubezpieczeniowej, Nr szkody, Dane dotyczące szkód ubezpieczeniowych Dane dotyczące odrzucenia szkody, Dane dotyczące wypowiedzenia umowy ubezpieczeniowej, Dane dotyczące wykupienia polisy ubezpieczeniowej na życie, Dane dotyczące reasekuracji / współubezpieczenia, Dane dotyczące ubezpieczenia społecznego (w zakresie niezbędnym dla linii ubezpieczeniowej), Osoba ubezpieczona, PESEL, Data urodzenia, Miejsce urodzenia, Dane biometryczne / dane dot. zdrowia, Zawód, Stanowisko w pracy, Destynacja / kierunek wyjazdu, Dochód, aktywa, kapitał, kapitał emerytalny, Dane dotyczące odrzucenia wniosków i szkód ubezpieczeniowych, Dane dotyczące płatności składek, Umowy w sprawie wynagrodzenia, Dane dotyczące prowizji, Nr pośrednika, Należności z tytułu anulowanej prowizji, Kredyty – zobowiązania, Skan dowodu osobistego / paszportu / dowodu rejestracyjnego, Skan prawa jazdy, Dane dotyczące wynagrodzeń osób Poszkodowanych, Nagrania zdarzenia (monitoring),	**WebBase:** Program informatyczny służący do przetwarzania danych odnoszących się do zawartych za pośrednictwem Athena umów ubezpieczenia wraz z danymi, które były wykorzystywane przy składaniu oferty ubezpieczeń, danymi odnoszącymi się do przebiegu umów ubezpieczenia włącznie ze sposobem ich zakończenia oraz płatności (składki, prowizje, odszkodowania) związanych z umowami ubezpieczenia wraz z historią zmian wprowadzanych przez użytkowników systemu. Istotnym elementem systemu jest możliwość przechowywania historii korespondencji związanej z daną umową ubezpieczenia lub danym podmiotem ubezpieczającym względnie ubezpieczonym. **Excel:** system do ewidencjonowania danych Klientów Spółki wraz z danymi umożliwiającymi wystawianie polis ubezpieczeniowych. **MIS:** system do prezentacji tych danych bez możliwości ich zmiany. Data Warehouse tworzący z danych zawartych w WebBase wielowymiarowe sekwencje odnoszące się do geografii, czasu, jednostki organizacyjnej, klientów itp. Celem działania systemu jest obrazowanie tendencji

		Dane biometryczne, Dane dotyczące zdrowia (dokumentacja medyczna), Dane dotyczące ubezpieczenia społecznego, Umowy o pracę lub potwierdzenia zatrudnienia, Numer polisy, Rozpoczęcie ubezpieczenia, Zakończenie ubezpieczenia, Numer roszczenia, Dane dotyczące odrzucenia roszczenia, Prowizja od zysku, Ubezpieczony, Dane dotyczące wyroków skazujących i naruszeń prawa,	rozwojowych portfela ubezpieczeń z uwzględnieniem czasu, miejsca, rodzaju klienta, typu ubezpieczenia i innych zmiennych, które łącznie i każda z osobna wpływają na portfel ubezpieczeń i mogą być pomocne w jego analizie, działaniach z zakresu controllingu i przy podejmowaniu decyzji zarządczych.
2.	Dane Pracowników i zleceniobiorców	Baza danych pracowników, zleceniobiorców, wykonawców umów o dzieło, osób zatrudnionych na podstawie kontraktów menedżerskich, pracowników tymczasowych, praktykantów, stażystów obejmująca następujące dane osobowe: **Dane podstawowe**, np.: Nr pracownika, Imię i nazwisko, Poprzednie nazwiska (lub ich części), Data urodzenia, Miejsce urodzenia, nr PESEL, nr dowodu tożsamości, Płeć, Stan rodzinny, Dzieci i inni członkowie rodziny, w odniesieniu do płatności innych, niż wynikających z zatrudnienia osoby, której dotyczą dane (w szczególności imię i nazwisko, data urodzenia, nr PESEL), Przedstawiciel prawny, Obywatelstwo, Adres zamieszkania, Prywatny nr telefonu i faksu oraz prywatny adres e-mail, Instytucja ubezpieczenia społecznego, Dane ubezpieczenia społecznego pracownika, Tytuł ubezpieczenia, Stopień pokrewieństwa pracownika, udział pracownika w spółce, Dane dotyczące kontynuacji wypłaty świadczenia, Podstawa do obliczenia składek, Przyczyna zakończenia stosunku pracy, Czas odprowadzania składek (od - do, miesiąc, rok, system księgowania), Tytuł ubezpieczenia, Potwierdzenie pracy i wynagrodzenia w celu uzyskania zasiłku chorobowego, Warunki pracy, Czynniki szkodliwe, Wymagania na danym stanowisku **Dane dot. zatrudnienia**, np.: Centrum/centra kosztów Stanowisko w spółce od – do, experience level, Przyczyny rozwiązania stosunku pracy, zdjęcie osoby, której dotyczą dane (dla identyfikatorów i zezwoleń)z Rejestracja czasu pracy, Dane dotyczące ewidencji i administrowania urlopami Data wypadku przy pracy, Okres pobytu w sanatorium i rehabilitacji, Urlop macierzyński (rozpoczęcie, zakończenie), Stopień niepełnosprawności wg Ustawy o zatrudnianiu osób niepełnosprawnych	**System kadrowy PIMS** - Główny system kadrowy Spółki do zarządzania danymi kadrowymi i płacowymi pracowników i zleceniobiorców. SAP: Główny system księgowy spółki do rejestracji zdarzeń finansowych związanych z prowadzoną działalnością. Jednocześnie jest to system do zarządzania płatnościami związanymi z zawartymi umowami ubezpieczenia.

		Dane dotyczące umowy (np. urlop roczny, miejsce pracy, data rozpoczęcia pracy, okres wypowiedzenia, data odejścia z pracy, powód odejścia z pracy, tygodniowy czas pracy itp. **Dane dotyczące wynagrodzeń** (na przykład płaca minimalna, premia za wyniki, premia za użytkowanie, wynagrodzenie podstawowe, świadczenia dodatkowe, dane o premiach itd. Obliczenie wynagrodzenia wg przepisów prawa, układów zbiorowych, regulacji spółki oraz umowy indywidualnej (wartościowanie stanowiska pracy), Wynagrodzenie brutto i netto (dane z miesięcznego paska wynagrodzeń), Odliczenie z wynagrodzenia netto z powodu przepisów prawnych lub regulacji spółki, Świadczenia dodatkowe, Składki na ubezpieczenie opłacane przez pracodawcę, Administrowanie zaliczkami i kredytami, Dane dotyczące zajęcia wynagrodzenia, Dane dotyczące deklaracji podatkowej na potrzeby rozliczenia podatku dochodowego, Oświadczenie z tytułu samotnego wychowywania dziecka lub bycia jedynym żywicielem rodziny (tak/nie), Urząd podatkowy osoby, której dotyczą dane, Dane dotyczące czasu pracy (np. tygodniowy czas pracy, nieobecności itd.)	
3.	Kandydaci	Dane kandydatów do pracy w Spółce: Imię i nazwisko, Poprzednie nazwiska (lub ich części), Data urodzenia, Miejsce urodzenia, Obywatelstwo, Płeć, Adres, Nr telefonu, E-mail, Zdjęcie, Informacje dotyczące wykształcenia i kwalifikacji, Umiejętności zawodowe i CV , Aplikacja kandydacka, Specjalne wymogi dotyczące zawodu, Wyniki badań medycyny pracy, Numer PESEL, Stanowisko w spółce, Warunki pracy, Czynniki szkodliwe, Wymagania na danym stanowisku, Wynagrodzenie, Centrum/centra kosztów, Job type (Rodzaj stanowiska), Experience level, Zaświadczenie o niepełnosprawności, Dane dowodu osobistego.	SAP: Główny system księgowy spółki do rejestracji zdarzeń finansowych związanych z prowadzoną działalnością. Jednocześnie jest to system do zarządzania płatnościami związanymi z zawartymi umowami ubezpieczenia.
4.	Płatnicy składki	Baza danych płatników składki wraz z danymi partnerów Spółki w zakresie wzajemnych płatności. Są to następujące dane osobowe: Imię i nazwisko, Adres, Nr telefonu, Nr telefonu komórkowego, Nr faksu, Adres e-mail, Płeć, Stan cywilny, Nazwisko rodowe, Obywatelstwo, Nr rachunku bankowego, Rodzaj	System do zarządzania danymi Active Directory

		ubezpieczenia (linia), Numer polisy, Data zawarcia polisy, Data ekspiracji polisy, Suma ubezpieczenia, Dane dot. składki, Data płatności składki, Numer szkody, Data rejestracji szkody, Data odrzucenia roszczenia, Data wypowiedzenia umowy ubezpieczenia, Podział prowizji, Dane dotyczące wykupu polis ubezpieczeniowych na życie, Dane dotyczące asekuracji / reasekuracji, Osoba ubezpieczona	
5.	Kontrahenci i dostawcy	Baza danych kontrahentów i dostawców wraz z danymi partnerów Spółki w zakresie wzajemnych płatności. Są to następujące dane osobowe: Nazwisko, Imię, Pan/Pani, Numer telefonu, Adres e-mail, nr rejestracyjny pojazdu	Exchange Server - System, za pomocą którego odbywa się komunikacja wewnątrz Spółek Grupy GrECo, do wszystkich tych spółek i od nich w zakresie poczty elektronicznej.
6.	Użytkownicy środowiska informatycznego	Baza danych użytkowników środowiska informatycznego Spółki wraz ze wszystkimi indywidualnymi uprawnieniami. Są to następujące dane osobowe: np. numer systemu, identyfikatory osobowe specyficzne dla danego obszaru, stosunek użytkownika systemu do administratora (np. stanowisko organizacyjne w firmie, pracownik, klient, procesor zamówień), identyfikator użytkownika i nazwa użytkownika, indywidualny kod dostępu i hasło (zaszyfrowane), okres ważności hasła / ostatnia zmiana / reset przez administratora systemu (administratora), prawa dostępu i ograniczenia, wymogi dotyczące nadawania uprawnień tajności (szkolenie, obowiązek zachowania tajemnicy danych), Daty spotkań i dostępność pracownika, Przypisane wyposażenie techniczne (sprzęt, oprogramowanie, notebooki, telefony komórkowe itp.), Centrum kosztowe i inne dane do rozliczeń Problem i rozwiązanie problemu (jak również numer zlecenia, data zlecenia, data rozwiązania problemu itp,) Autoryzacje dostępu do systemów , Informacje o przekierowaniu wiadomości po zakończeniu stosunku pracy.	

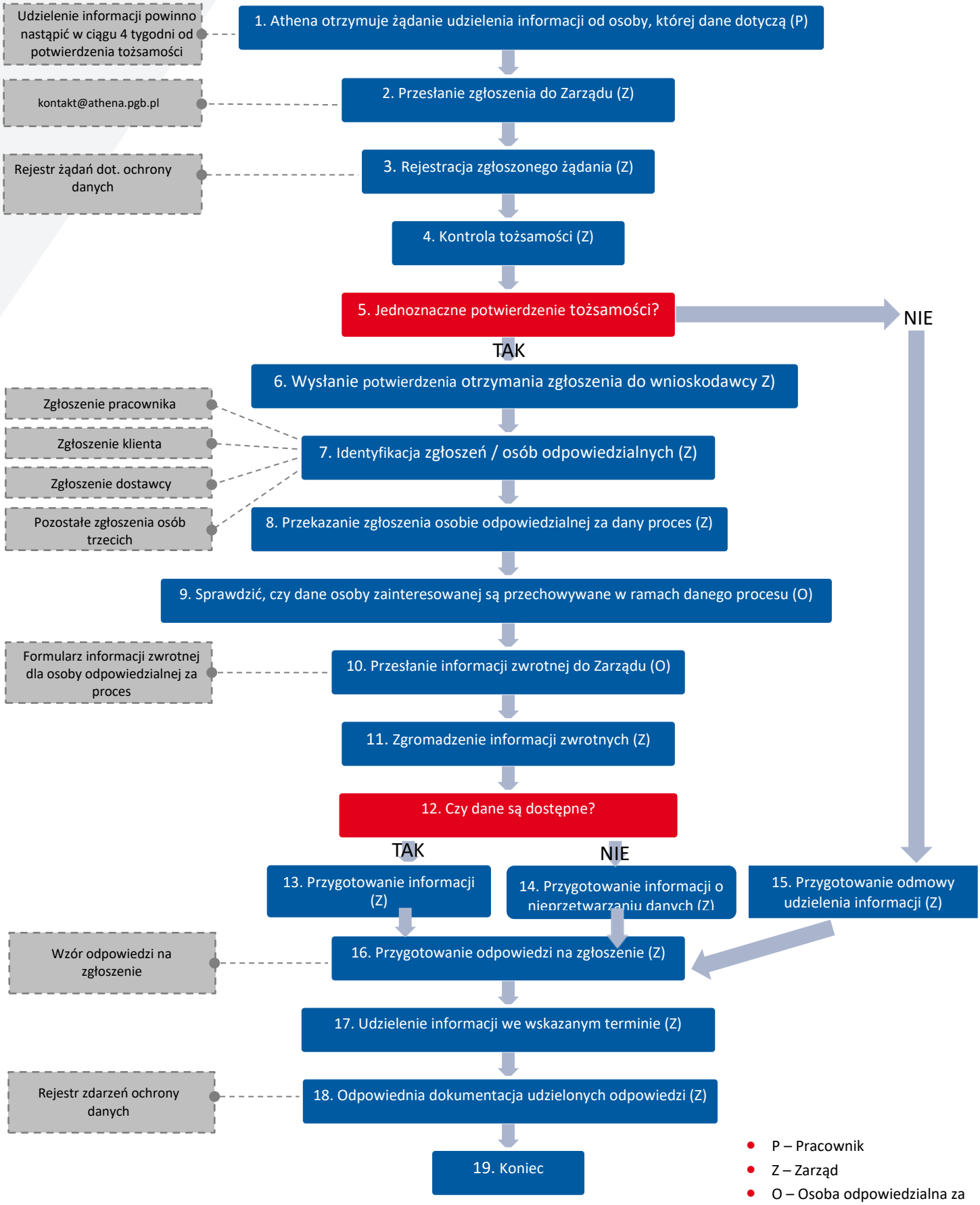
7.	Użytkownicy poczty elektronicznej	Baza danych użytkowników, adresatów i nadawców poczty elektronicznej, dane osobowe typu: Dane podstawowe, np.: Nr pracownika, Imię i nazwisko, Prywatny nr telefonu i faksu oraz prywatny adres e-mail, Dane dot. zatrudnienia, np.: Centrum/centra kosztów Stanowisko w spółce od – do, experience level,

Załącznik nr 2 – Rejestry czynności przetwarzania danych

Rejestry czynności przetwarzania opisane są w odrębnych plikach:

- Rejestr dotyczący systemu MIS
- Rejestr dotyczący systemu PIMS
- Rejestr pionu Księgowości i Administracji (F&A)
- Rejestr Pionu Revenue Management (RM)
- Rejestr Pionu HR (Zarządzanie personelem i Rozwój pracowników)
- Rejestr Pionu IA (Rewizja wewnętrzna i system dotyczący sygnalistów)
- Rejestr dotyczący poczty elektronicznej i systemów IT
- Rejestr dotyczący bazy spotkań
- Rejestr dotyczący współpracy z Dostawcami
- Rejestr dotyczący pośrednictwa ubezpieczeniowego (S&AM / RIT)
- Rejestr dotyczący marketingu.

Załącznik nr 3 - Procedura udzielenia informacji na żądanie.



- P – Pracownik
- Z – Zarząd
- O – Osoba odpowiedzialna za proces

Załącznik nr 4 – Wzór pisma „Udzielenie informacji zgodnie z art. 15 RODO

Athena Sp. z o.o.

ul. Winklera18
60-246 Poznań
www.athena.pgb.pl

NIP 782-20-29-074,
REGON: 631047533
VIII Wydział Gospodarczy KRS
KRS 0000166079

Kapitał zakładowy 60.000 zł
Nr zezwolenia 452
nr konta: 82 1090 1450 0000 0000 4502 4530

Sz. P. Imię i nazwisko

ul.....

kod pocztowy, miasto

Poznań, dnia .... 2022 roku

Dotyczy: Udzielenie informacji zgodnie z art. 15 RODO

Szanowny Panie / Szanowna Pani

1. W dniu [data] otrzymaliśmy Pana/Pani prośbę o udzielenie informacji zgodnie z art. 15 RODO. Pana/Pani tożsamość została potwierdzona w wystarczającym stopniu.

2. {W przypadku odpowiedzi udzielanej w przewidzianym terminie} Odpowiadamy na Pani/Pana wniosek w terminie przewidzianym w Rozporządzeniu.

{W przypadku przedłużenia terminu zgodnie z Art. 12 ust. 3 RODO}

Zgodnie z pismem z dnia [data] skorzystaliśmy z możliwości przedłużenia terminu do trzech miesięcy ze względu na [złożoność wniosku lub liczbę wniosków, co wymaga bardziej szczegółowego uzasadnienia].

3. {jeżeli żadne dane nie są przetwarzane} Nie przetwarzamy żadnych danych osobowych, które Pani/Pana dotyczą. {tu dalej tekst Nr 9}.

{Jeżeli dane są przetwarzane} Przetwarzamy następujące dane osobowe, które Pani/Pana dotyczą:

[należy podać wykaz danych, które rzeczywiście są przetwarzane].

W załączniku znajdują się wydruki dotyczące przetwarzanych danych.

4. Dane te są przetwarzane w następujących celach: [Należy wymienić cele włącznie z podstawą prawną]

5. {jeśli dane są przekazywane} Dane są przekazywane do następujących odbiorców: [należy podać odbiorców lub kategorie odbiorców, włącznie z państwem, w którym mieści się ich siedziba].

{jeżeli dane są przekazywane do państw trzecich} Przekazywanie danych odbiorcom znajdującym się w państwie trzecim opiera się na następujących zabezpieczeniach: [należy uzupełnić zabezpieczenia]

6. Przechowujemy Pani/Pana dane. [Należy podać planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu].

7. { jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą}: Otrzymaliśmy Pani/Pana dane od [należy podać dostępne informacje dot. pochodzenia danych, np. adres spółki XY].

8. {jeśli ma zastosowanie} Korzystamy z procedur zautomatyzowanego podejmowania decyzji / profilowania, które mają dla Pani/Pana skutki prawne lub znacząco wpływają na przetwarzane Pani/Pana dane osobowe.: [proszę podać istotne informacje na temat zastosowanej logiki, jak również zakresu i zamierzonych konsekwencji].

9. Przysługuje Panu/Pani prawo do sprostowania, usunięcia, ograniczenia i prawo do cofnięcia zgody. W związku z tym prosimy o kontakt, jeśli chce Pan/Pani skorzystać z tych praw. Jeśli uważa Pan/Pani, że przetwarzanie danych narusza prawo o ochronie danych lub Pana/Pani dane osobowe zostały w jakikolwiek inny sposób naruszone, ma Pan/Pani prawo do wniesienia skargi do UODO.

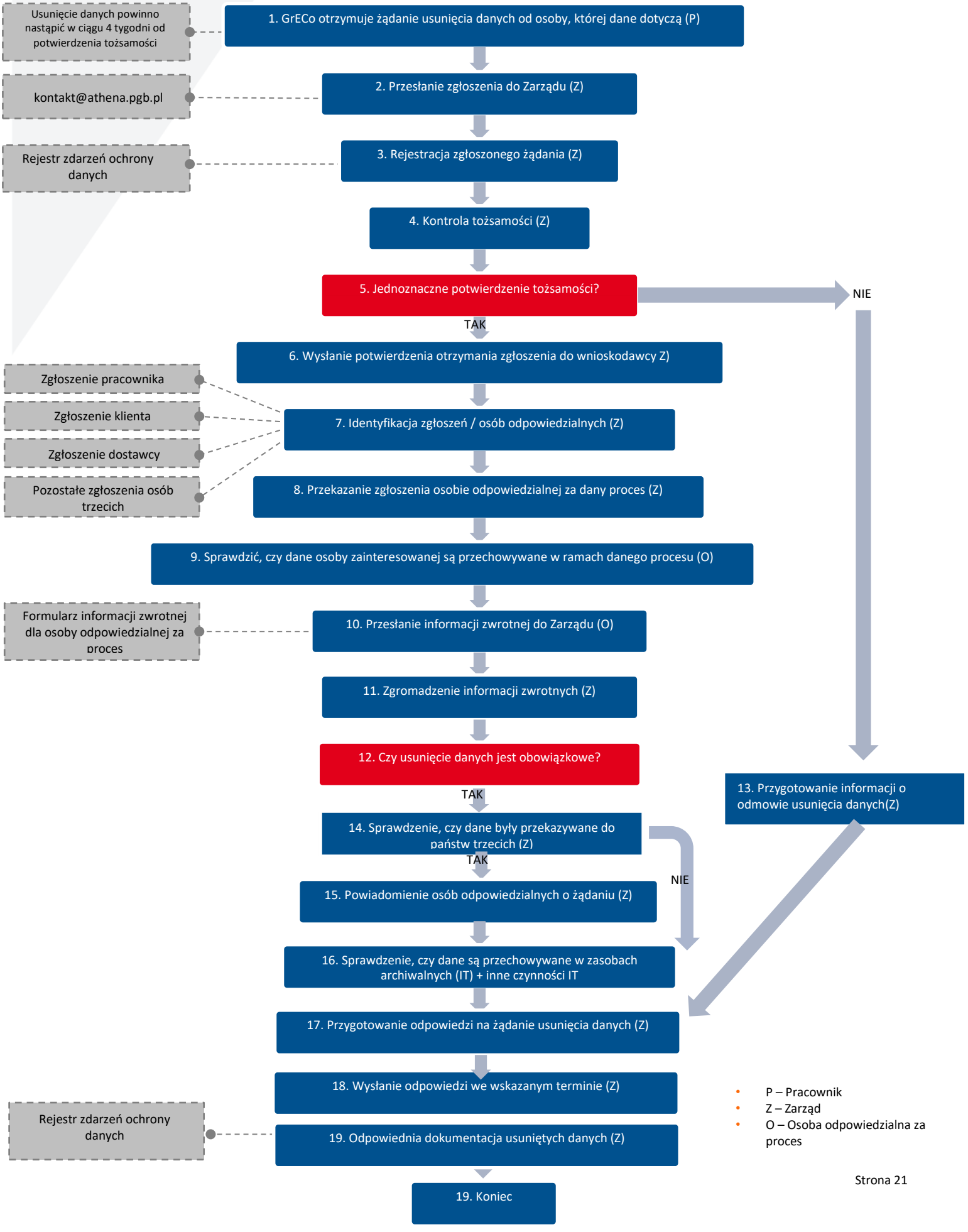
Z poważaniem

Jacek Bobiński
Prezes Zarządu

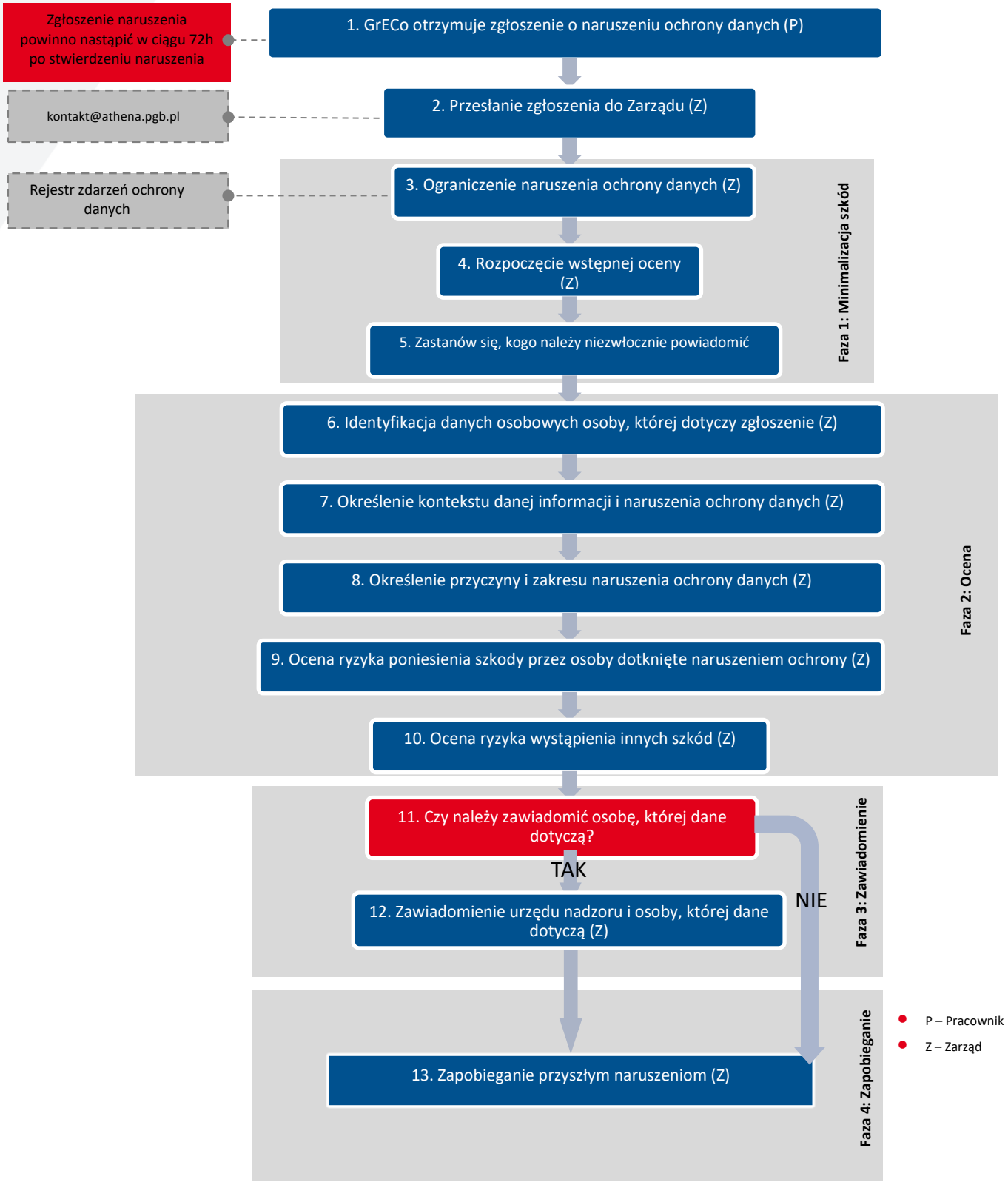
Załącznik nr 5 – Rejestr żądań dotyczących ochrony danych.

Lp	Data wpływu	Oznaczenie osoby składającej żądanie	Przedmiot żądania	Sposób jego realizacji	Termin przesłania zawiadomienia o realizacji	Przyczyna odmowy	Sposób przesłania zawiadomienia	Osoba realizująca czynności dot. żądania
1								
2								
3								

Załącznik nr 6 - Procedura usunięcia danych na żądanie



Załącznik nr 7 – Procedura zarządzania naruszeniami ochrony danych osobowych.



Załącznik nr 8 – Rejestr naruszeń ochrony danych osobowych.

Lp	Opis incydentu	Źródło zgłoszenia	Data rozpoczęcia	Data zakończenia	Osoba odpowiedzialna	Przyczyna incydentu	Działania korygujące (naprawcze)
1							
2							
3							

Załącznik nr 9 – Procedura przetwarzania danych osobowych

I. POSTANOWIENA OGÓLNE

§ 1. Przedmiot regulacji

1. Niniejsza procedura określa zasady przetwarzania danych osobowych w Athena Spółka z ograniczoną odpowiedzialnością, zwaną dalej Administratorem Danych.
2. Przez przetwarzanie danych osobowych rozumie się jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie w sposób zautomatyzowany lub niezautomatyzowany. .
3. Postanowienia Procedury odnoszą się do wszystkich osób będących pracownikami Administratora Danych lub osób świadczących usługi na rzecz Administratora Danych i posiadających dostęp do danych osobowych.

§ 2. Regulacje

Przy przetwarzaniu danych osobowych należy przestrzegać postanowień Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, postanowień Ustawy o ochronie danych osobowych z dnia 24 maja 2018 roku oraz wewnętrznych regulacji obowiązujących u Administratora Danych i innych ustaw związanych z wykonywaną przez Administratora Danych działalnością.

II. POSTANOWIENIA SZCZEGÓLNE

§ 3. Przetwarzane dane

1. Administrator Danych przetwarza dane osobowe wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim spełniony jest co najmniej jeden z poniższych warunków:
    a. osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
    b. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
    c. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
    d. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej.
2. Zgoda osoby, której dane dotyczą, musi być dobrowolna, świadoma i jednoznaczna. Wykonanie umowy nie może być uzależnione od zgody na przetwarzanie danych
3. Przetwarzając dane osobowe na podstawie zgody osoby, której dane dotyczą, należy spełnić następujące warunki:
    a. zgoda musi zostać wyrażona przed planowanym przetwarzaniem danych
    b. zgoda może zostać udzielona na piśmie, w formie elektronicznej lub ustnej.
    c. osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.

d. Zgoda nie musi się ograniczać do jednego celu przetwarzania danych, może dotyczyć kilku celów przetwarzania danych. Muszą one jednak być jasno opisane, zdefiniowane i uzasadnione, tak aby dane osobowe były przetwarzane tylko w celu, do którego zostały zgromadzone.

4. Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby, chyba że:
   a. osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach,
   b. przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej
   c. przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
   d. przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;

§ 4. Przetwarzanie danych osobowych

1. Dane osobowe muszą być zawsze przetwarzane zgodnie z prawem, w sposób rzetelny i przejrzysty, transparentny i prawidłowy. Zakres przetwarzanych danych musi być ograniczony do niezbędnego minimum. Przetwarzanie danych musi odbywać się w sposób zapewniający odpowiednie bezpieczeństwo danych.
2. Administrator Danych przetwarza dane osobowe wyłącznie w celu, w jakim zostały zgromadzone.
3. Dane osobowe przetwarzane są w systemie tradycyjnym, bez wykorzystania systemów informatycznych oraz w systemach informatycznych.
4. Dane osobowe przetwarzane są w wydzielonych do tego pomieszczeniach.
5. Dokumenty zawierające dane osobowe przechowywane są w wydzielonych pomieszczeniach w szafach zamkniętych na klucz albo w szafach pancernych.

§ 6. Osoby przetwarzające dane osobowe

1. Osobami uprawnionymi do przetwarzania danych osobowych są pracownicy Administratora Danych oraz inne osoby, którym powierzono przetwarzanie danych osobowych, które:
   1) posiadają upoważnienie wydane przez Administratora Danych
   2) podpisały oświadczenie o zachowaniu w poufności i tajemnicy przetwarzanych danych osobowych.
2. Zabrania się przetwarzania danych osobowych:
   1) osobom, które nie posiadają upoważnienia wydanego przez Administratora Danych,
   2) osobom, które posiadają upoważnienie Administratora Danych, ale przetwarzanie przez nie danych w danym momencie jest nieuzasadnione.

§ 7. Odpowiedzialność za przetwarzanie danych

1. Osobami odpowiedzialnymi za przetwarzane danych są osoby przetwarzające dane oraz przełożeni tych osób.
2. O jakichkolwiek nieprawidłowościach powstałych przy przetwarzaniu danych, informuję się Administratora Danych, który dokonuje oceny stanu faktycznego i w razie konieczności stosuje odpowiednie środki zapobiegawcze.

§ 8. Obowiązki Administratora Danych

1. Administrator Danych zapewnia, aby dane osobowe były:
   1) przetwarzanie zgodnie z prawem, w szczególności z RODO, ustawą o ochronie danych osobowych i innymi ustawami związanymi z prowadzoną przez Administratora Danych działalnością.
   2) zbierane w celach związanych z prowadzoną przez Administratora Danych działalnością,
   3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane, w szczególności poprzez dołożenie należytej staranności, aby dane osobowe były zgodne z prawdą, kompletne i nie wykraczające poza potrzeby wynikające z celu ich zbierania,
   4) przechowywane nie dłużej niż jest to niezbędne do osiągnięcia celu ich przetwarzania.
   Administrator Danych zapewnia kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

2. Administrator danych wdraża odpowiednie środki techniczne i organizacyjne w celu wykazania, że przetwarzanie danych odbywa się zgodnie z Rozporządzeniem.

§ 9. Archiwizowanie danych osobowych

1. Dane osobowe są przechowywane do momentu osiągnięcia celu, dla którego były przechowywane.
2. Dane osobowe, co do których ustał cel ich przetwarzania, są usuwane w trwały sposób, albo pozbawiane cech identyfikujących poprzez ich anonimizację.

§ 10. Udostępnianie danych osobowych

1. Przed udostępnieniem danych osobowych, Administrator Danych bada zasadność żądania oraz cel, dla jakiego będą dane osobowe przetwarzane przez ubiegającego się o udostępnienie danych osobowych.
2. W przypadku udostępnienia danych osobowych, Administrator Danych odbiera oświadczenie od podmiotu, któremu przekazuje dane osobowe, w którym zobowiązuje się on do posługiwania danymi osobowymi do tych samych celów, co Administrator Danych.

§ 11. Powierzenie przetwarzania danych osobowych

1. Administrator danych może powierzyć innemu podmiotowi, w drodze pisemnej umowy o powierzenie przetwarzania danych osobowych.
2. Administrator korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi Rozporządzenia i chroniło prawa osób, których dane dotyczą.
3. Podmiot, o którym mowa w ust. 1 może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

§ 12. Prowadzone ewidencje

1. Administrator Danych prowadzi ewidencję osób upoważnionych do przetwarzana danych osobowych zgodnie z załącznikiem nr 1 do niniejszej Procedury.

§ 13. Wątpliwości

W przypadku wątpliwości co do legalności przetwarzania albo przekazywania danych osobowych, pracownik zwraca się do Administratora Danych o zajęcie stanowiska. Do czasu rozstrzygnięcia sprawy, dane osobowe nie mogą być przetwarzane ani przekazywane.

III. POSTANOWIENIA KOŃCOWE

§ 14. Nadzór

Nadzór nad przetwarzaniem danych osobowych sprawuje Zarząd Administratora Danych.

§ 15. Wejście w życie

Niniejsza procedura została przyjęta uchwałą Zarządu w dniu 25 maja 2018 roku i obowiązuje od dnia przyjęcia.

Załącznik nr 1 do Procedury przetwarzania danych osobowych w Athena Spółka z ograniczoną odpowiedzialnością – wzór ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych

Lp.	Imię i nazwisko	stanowisko	Zakres upoważnienia	Identyfikator w systemie informatycznym	Data wpisu	Data wykreślenia

Załącznik nr 10 – Środki bezpieczeństwa (organizacyjne i techniczne) ochrony danych.

Środki bezpieczeństwa ochrony danych opisane są w odrębnym pliku „General_TOM_Athena”.

Załącznik nr 11 – Wzór zgody na przetwarzanie danych osobowych dotyczących zdrowia.

Zgoda na przetwarzanie danych osobowych dotyczących zdrowia

I. Informacje ogólne

Zgodnie z przepisami ogólnego Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO) dane osobowe to wszystkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Może tu chodzić o informacje prywatne, służbowe, gospodarcze, czynniki określające fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby. Dane osobowe to zatem w szczególności imię i nazwisko, data urodzenia, adres, płeć, numer telefonu, numer rejestracyjny pojazdu, numer polisy, ale także dane dotyczące zdrowia.

W myśl Art. 9 RODO dane dotyczące zdrowia są szczególnie chronione, a ich przetwarzanie jest zabronione, chyba że osoba, której dane dotyczą, wyrazi na to zgodę.

Przetwarzanie i rejestrowanie Państwa danych medycznych w ramach obowiązującej nas Umowy jest niezbędne do oceny i zawarcia ochrony ubezpieczeniowej, a także do wypełnienia zobowiązań wobec ubezpieczyciela.

Wyrażona przez Państwa zgoda może być wycofana w dowolnym momencie.

II. Zgoda na przetwarzanie danych

1. Niniejszym wyrażam zgodę na przetwarzanie moich danych osobowych dotyczących stanu zdrowia przez Athena Sp. z o.o. (Członka Grupy GrECo) z siedzibą w Poznaniu (60-246), ul. Winklera 18, zarejestrowaną w Sądzie Rejonowym w Poznaniu, VIII Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS: 0000166079, NIP: 782-20-29-074, REGON: 631047533, kapitał zakładowy 60.000 zł, w celu pośrednictwa w zawarciu i wykonaniu umowy ubezpieczenia.
2. Wyrażam zgodę na udostępnianie ww. danych Spółce GrECo International Holding AG z siedzibą w Wiedniu (Austria) jako spółce zarządzającej i kontrolującej oraz świadczącej usługi IT dla całej Grupy GrECo, a także Towarzystwom Ubezpieczeniowym w celu i zakresie niezbędnym do zawarcia i wykonywania umowy ubezpieczenia, w tym w sprawach o odszkodowanie.
3. Podaję dane osobowe dobrowolnie i oświadczam, że są one zgodnie z prawdą. Zapoznałem(-am) się z treścią klauzuli informacyjnej, w tym z informacją o celu i sposobach przetwarzania danych osobowych oraz prawie dostępu do treści swoich danych i prawie ich poprawienia.
4. Oświadczam jednocześnie, że zostałem poinformowany, że mogę w dowolnym momencie wycofać zgodę na przetwarzanie moich danych oraz że wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

_____

(miejsce, data)

_____

(Imię i nazwisko oraz podpis osoby składającej oświadczenie)

Załącznik nr 12 – Wzór zgody na przetwarzanie danych biometrycznych.

Zgoda na przetwarzanie danych biometrycznych

I. Informacje ogólne

Zgodnie z przepisami ogólnego Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO) dane osobowe to wszystkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Może tu chodzić o informacje prywatne, służbowe, gospodarcze, czynniki określające fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby. Dane osobowe to zatem w szczególności imię i nazwisko, data urodzenia, adres, płeć, numer telefonu, numer rejestracyjny pojazdu, numer polisy, ale także dane biometryczne (czyli dowód tożsamości ze zdjęciem oraz informacją o kolorze oczu czy wzroście).

W myśl Art. 9 RODO dane biometryczne są szczególnie chronione, a ich przetwarzanie jest zabronione, chyba że osoba, której dane dotyczą, wyrazi na to zgodę.

Przetwarzanie i rejestrowanie Państwa danych osobowych w ramach obowiązującej nas Umowy jest niezbędne do rozpatrzenia roszczenia, a także do wypełnienia zobowiązań wobec ubezpieczyciela.

Wyrażona przez Państwa zgoda może być wycofana w dowolnym momencie.

II. Zgoda na przetwarzanie danych

1. Niniejszym wyrażam zgodę na przetwarzanie moich danych osobowych dotyczących stanu zdrowia przez Athena Sp. z o.o. (Członka Grupy GrECo) z siedzibą w Poznaniu (60-246), ul. Winklera 18, zarejestrowaną w Sądzie Rejonowym w Poznaniu, VIII Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS: 0000166079, NIP: 782-20-29-074, REGON: 631047533, kapitał zakładowy 60.000 zł, w celu pośrednictwa w zawarciu i wykonaniu umowy ubezpieczenia.
2. Wyrażam zgodę na udostępnianie ww. danych Spółce GrECo International Holding AG z siedzibą w Wiedniu (Austria) jako spółce zarządzającej i kontrolującej oraz świadczącej usługi IT dla całej Grupy GrECo, a także Towarzystwom Ubezpieczeniowym w celu i zakresie niezbędnym do rozpatrzenia roszczenia.
3. Podaję dane osobowe dobrowolnie i oświadczam, że są one zgodnie z prawdą. Zapoznałem(-am) się z treścią klauzuli informacyjnej, w tym z informacją o celu i sposobach przetwarzania danych osobowych oraz prawie dostępu do treści swoich danych i prawie ich poprawienia.
4. Oświadczam jednocześnie, że zostałem poinformowany, że mogę w dowolnym momencie wycofać zgodę na przetwarzanie moich danych oraz że wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

_____

(miejsce, data)

_____

(Imię i nazwisko oraz podpis osoby składającej oświadczenie)

Załącznik nr 13 – Polityka prywatności.

Polityka prywatności opisana jest w odrębnym pliku „Athena_Polityka_Prywatnosci.pdf”.

Athena Sp. z o.o.

ul. Winklera 18 | 60-246 Poznań
Tel. +48 501 098 338| Tel. +48 516 020 282| athena@athena.pgb.pl
NIP: 782-20-29-074 | REGON: 631047533| Kapitał zakładowy 60.000 zł | Licencja PUNU 452
www.athena.pgb.pl