POLITYKA
BEZPIECZEŃSTWA
ASAP POLSKA SP. Z O.O.
(ASAP)

DEFINICJE

§1

Ilekroć w niniejszym dokumencie jest mowa o:

1. Administratorze Danych (AD) - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, decydujące o celach i środkach przetwarzania danych osobowych.
2. Prezesie - rozumie się przez to Prezesa Zarządu ASAP.
3. Inspektorze Danych Osobowych (IDO) - oznacza osobę odpowiedzialną za bezpieczeństwo przetwarzania informacji oraz za podejmowanie odpowiednich działań w przypadku wykrycia nieprawidłowości w systemie zabezpieczeń, o której mowa w art. 37-39 RODO.
4. Administratorze Systemów Informatycznych (ASI) - rozumie się przez to współpracownika ASAP nadzorującego z upoważnienia działanie i prace systemów informatycznych.
5. Danych osobowych - rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
6. Haśle - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym Administratora Danych.
7. Identyfikatorze użytkownika - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
8. Odbiorcy danych - oznacza 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.
9. Przetwarzającym - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora.
10. Przetwarzaniu danych - rozumie się przez to 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.
11. Pseudonimizacja - polega na takim zmodyfikowaniu zbioru danych, aby niemożliwe stało się przypisanie znajdujących się tam informacji do konkretnych osób oraz ich zidentyfikowanie.
12. RODO oznacza Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 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).

13. Sieci publicznej - rozumie się przez to sieć publiczną w rozumieniu art.2pkt.28 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne.
14. Sieci teleinformatycznej - rozumie się przez to służące do przetwarzania danych osobowych organizacyjnie i technicznie systemy teleinformatyczne wraz z łączącymi je urządzeniami i liniami.
15. Sieci telekomunikacyjnej - rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt.35 ustawy z dnia 16 lipca 2004 r. Pławo telekomunikacyjne (DZ.U.2004.171.1800).
16. Danych - rozumie się przez sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń za pomocą których przetwarzane są dane osobowe
17. Usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
18. Uwierzytelnianiu - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
19. Użytkowniku - rozumie się przez to upoważnionego przez Administratora danych (w przypadku powołania Inspektora Danych Osobowych również przez IDO), wyznaczonego do przetwarzania danych osobowych pracownika, który odbył stosowne szkolenie w zakresie ochrony tych danych.
20. Zabezpieczeniu danych w systemie informatycznym - rozumie się przez to wdrożenie i eksploatację adekwatnych środków technicznych i organizacyjnych spośród stosowanych w ASAP zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
21. Zabezpieczeniu systemu informatycznego - rozumie się przez to wdrożenie stosowanych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą.
22. Zbiorze danych - rozumie się przez uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

POSTANOWIENIA OGÓLNE

§ 1

1. Administratorem Danych Osobowych jest ASAP Polska sp. z o.o. ul. Komitetu Obrony Robotników 72, 02-146 Warszawa, KRS 0000582265, NIP 522-304-20-67
2. Zasady określone w niniejszej Polityce Bezpieczeństwa Informacji (zwanej dalej: „Polityką") wynikają z przepisów o ochronie danych osobowych przyjętych w RODO.

3. Polityka powinna zostać wdrożona w działalności ASAP sp. z o.o. („**ASAP**"), aby zapewnić poziom ochrony informacji i danych osobowych odpowiedni do potencjalnych zagrożeń. Uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających dane osobowe, a przede wszystkim zapewnienie ochrony danych osobowych przetwarzanych w nazwa podmiotu przed wszelkiego rodzaju zagrożeniami, tak zewnętrznymi jak i wewnętrznymi.
4. Polityka określa środki techniczne i organizacyjne niezbędne do zachowania zasad przetwarzania informacji w tym danych osobowych zgodnych z RODO tj.
   - zgodności z prawem, rzetelności i przejrzystości,
   - zasada ograniczenia celu przetwarzania danych,
   - zasada minimalizacji danych,
   - zasada prawidłowości danych,
   - zasada ograniczenia przechowania danych,
   - zasada integralności i poufności danych,
   - zasada rozliczalności.
5. Celem Polityki Bezpieczeństwa przetwarzania danych osobowych w ASAP jest:
   a) uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających dane osobowe, a przede wszystkim zapewnienie ochrony danych osobowych przetwarzanych w ASAP przed wszelkiego rodzaju zagrożeniami, tak zewnętrznymi jak i wewnętrznymi.
   b) wskazanie działań, jakie należy podejmować-aby prawidłowo zabezpieczyć dane osobowe.
   c) Ustalenie wewnętrznych procedur: na wypadek naruszenia danych osobowych oraz realizacji praw osób których dane osobowe są przetwarzane zgodnie z RODO.

§2

Polityka Bezpieczeństwa została tworzona w związku z wymaganiami zawartymi w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 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) i stanowi zbiór zasad i wewnętrznych regulacji jakie są stosowane w ASAP w celu przetwarzania danych osobowych zgodnie z prawem.

§ 3

Obszarem przetwarzania danych osobowych są wydzielone pomieszczenia w budynku, w którym mieści się ASAP.

§ 4

Ochrona danych osobowych realizowana jest poprzez stosowanie zabezpieczeń fizycznych, informatycznych oraz procedur organizacyjnych zapewniających rozliczalność ich zastosowania do ilości oraz wagi przetwarzanych przez ASAP danych osobowych.

§ 5

Polityka Bezpieczeństwa zawiera zbiór działań, zmierzających do uzyskania i utrzymania ustalonego już na etapie zbierania danych osobowych poziomu bezpieczeństwa danych osobowych oraz:

1. Poufności danych - rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom.
2. Integralności danych - rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
3. Rozliczalności danych - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie.
4. Dostępności informacji - rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne.
5. Zarządzania ryzykiem - rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

§6

Polityka Bezpieczeństwa zapewnia:

1. Spójność z wyznaczonymi zadaniami.
2. Skuteczniejsze działania w odniesieniu do zagrożeń poufności, integralności i dostępności danych osobowych.
3. Realizację zadań w taki sposób, aby podnieść jakość i wiarygodność przede wszystkim w stosunku do osób fizycznych ale również wobec kontrahentów oraz partnerów biznesowych.
4. Ochronę danych osobowych tworzonych, przetwarzanych, przechowywanych i przesyłanych nie tylko pomocą systemów informatycznych ale również w innych obszarach ich przetwarzania i przechowywania (np. w wersji papierowej).

§7

1. W zbiorach Administratora Danych przetwarzane są dane zwykłe, (m. in. adres zamieszkania, numer PESEL) oraz tzw. Szczególna Kategoria Danych Osobowych o których mowa w art. 9 RODO (np. informacje dotyczące stanu zdrowia)
2. Zbiory danych są przetwarzane i składowane zarówno w postaci dokumentacji tradycyjnej jak i w

formie elektronicznej.

3. Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych w ASAP jak i w przypadku innych osób współpracujących np. stażystów, praktykantów.

ORGANIZACJA PRZETWARZANIA DANYCH OSOBOWYCH

§1

1. Osoba uprawniona do reprezentowania Administratora Danych realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:
   a) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi jej obowiązków,
   b) odwołuje upoważnienia do przetwarzania danych osobowych lub usuwa konta użytkownika z systemu informatycznego,
   c) prowadzi ewidencje osób upoważnionych do przetwarzania danych osobowych.
   d) wyznacza Inspektora Danych Osobowych oraz określa zakres jego zadań i czynności,
   e) zgłasza powołanie i odwołanie Inspektora Danych Osobowych do Generalnego Inspektora Danych Osobowych (Prezesa Urzędu Ochrony) lub innego organu nadzorczego oraz odpowiada za terminowe zgłoszenie powołania i odwołania Inspektora Danych Osobowych
   f) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszeń procedur bezpiecznego przetwarzania danych osobowych.
   b) wyznacza do prowadzenia nadzoru nad działaniem i zabezpieczeniem wykorzystywanych systemów informatycznych.
   c) przeprowadza okresową analizę ryzyka przetwarzania danych osobowych i w razie potrzeby wnioskuje do Administratora a zmianę/modyfikację ilości przetwarzanych danych lub stosowanych zabezpieczeń zgodnie z zasadą adekwatności.
2. Osobą uprawnioną do reprezentowania Administratora Danych jest Prezes Zarządu.

§ 2

Inspektor Danych Osobowych (IDO) realizuje zadania w zakresie nadzoru nad przestrzeganiem zasad ochrony danych osobowych, w tym zwłaszcza:

1. Sprawuje nadzór nad zastosowaniem środków technicznych, a także organizacyjnych w celu zapewnienia bezpieczeństwa danych.
2. Sprawuje nadzór nad funkcjonowaniem systemu zabezpieczeń, w tym także nad prowadzeniem ewidencji z zakresu ochrony danych osobowych.
3. Koordynuje wewnętrzne kontrole przestrzegania przepisów o ochronie danych osobowych.

4. Prowadzi korespondencję z Generalnym Inspektorem Ochrony Danych Osobowych.
5. Nadzoruje prowadzenie dokumentacji z zakresu ochrony danych osobowych.
6. Przygotowuje materiały szkoleniowe z zakresu ochrony danych osobowych i prowadzi szkolenia ogólne osób upoważnionych do przetwarzania danych osobowych w tym szkoleń osób upoważnionych z zakresu przetwarzania danych osobowych w systemach informatycznych
7. Prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym.
8. Podejmuje zgodnie z RODO odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia systemu informatycznego tj. zgłasza naruszenie do organy nadzorczego w ciągu 72 godzin i w razie konieczności informuje o tym osoby których dane zostały naruszone lub sporządza notatkę dlaczego takie zgłoszenie nie jest wymagane.
9. Sprawdza zgodność przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowuje w tym zakresie sprawozdania dla Prezesa Zarządu.
10. Nadzoruje opracowanie i aktualizowanie wewnętrznych zasad oraz dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną oraz przestrzegania zasad w niej określonych.
11. Zapewnia zapoznanie się osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
12. Współpracuje z organem nadzorczym w sprawach dotyczących przetwarzania danych osobowych w ASAP.
13. Reprezentuje ASAP w kontaktach z osobami których dane są przetwarzane, przyjmuje i rozpatruje sprzeciwy tych osób dotyczące przetwarzania ich danych osobowych, wykonuje wnioskowane przez nie czynności takie jak np. usuwa, zmienia, przenosi do innego administratora dane osobowe.

§3

W przypadku niepowołania Inspektora Danych Osobowych, jego zadania wykonuje osoba uprawniona do reprezentowania Administratora Danych.

§4

1. W przypadku niewyznaczenia Administratora Systemu Informatycznego (ASI) jego zadania może wykonywać na podstawie zawartej umowy podmiot zewnętrzny świadczący usługi w branży informatycznej.
2. Umowa z takim podmiotem musi zawierać co najmniej klauzule poufności dotyczącą budowy, funkcjonowania oraz zabezpieczenia Systemów informatycznych oraz klauzule powierzenia przetwarzania danych osobowych lub osobną umowę powierzenia przetwarzania danych osobowych

w przypadku gdy taki podmiot będzie miał dostęp do danych osobowych.

§5

Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana przestrzegać następujących zasad:

1. Może przetwarzać dane osobowe wyłącznie w zakresie w ustalonym upoważnieniu i tylko w celu wykonywania nałożonych na nią obowiązków.
2. Rozwiązanie stosunku pracy bądź odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych.
3. Musi zachować tajemnicę danych osobowych oraz przestrzegać procedur ich bezpiecznego przetwarzania.
4. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u Administratora Danych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji.
5. Zapoznaje się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej Polityki Bezpieczeństwa.
6. Stosuje określone u Administratora Danych wytyczne i procedury mające na celu przetwarzanie danych osobowych zgodnie z obowiązującym prawem.
7. Korzysta z systemu informatycznego Administratora Danych w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników.
8. Zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym w sposób określony przez Administratora Danych.

§6

W ASAP prowadzone są następujące rejestry i ewidencje wchodzące w skład dokumentacji z zakresu ochrony danych osobowych:

1. Rejestr czynności przetwarzania danych osobowych
2. Ewidencja osób upoważnionych do przetwarzania danych osobowych.
3. Ewidencja zbiorów danych.
   Ponadto mogą zostać wprowadzone.
4. Ewidencja pozyskanych zgód na przetwarzanie danych osobowych.
5. Ewidencja osób posiadających dostęp do pomieszczeń Administratora Danych (rejestr kluczy, rekordy wejść i wyjść).
6. Ewidencja zawartych prze ASAP umów powierzenia przetwarzania danych osobowych.

WYKAZ POMIESZCZEŃ TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

§1

Pomieszczeniami tworzącymi obszar, w którym przetwarzane są dane osobowe są pomieszczenia, w których znajdują się zbiory danych w formie kartotek, rejestrów, baz danych, wpisów tymczasowych, informacji roboczych zawierających w rozumieniu RODO dane osobowe.

§2

Pomieszczeniami tworzącymi obszar, w którym przetwarzane są dane osobowe są również pomieszczenia, w których znajduje się stacjonarny lub przenośny sprzęt komputerowy (stacje robocze), na których lub za których pomocą przetwarzane są dane osobowe.

§3

Przebywanie w pomieszczeniach znajdujących się wewnątrz obszaru, o którym mowa w § 1 i 2 osób nieuprawnionych do dostępu do danych osobowych, jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych, posiadającej upoważnienie do przetwarzania danych.

§4

Pomieszczenia lub miejsca, w których przetwarzane są dane osobowe powinny być chronione na czas nieobecności w nich osób upoważnionych do przetwarzania danych osobowych, w sposób uniemożliwiający dostęp do nich osób niepowołanych.

§5

Wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe został określony w załączniku nr 1 do niniejszej Polityki Bezpieczeństwa. Wykaz ten został stworzony w celach realizacji zasady rozliczalności przetwarzani danych osobowych.

WYKAZ ZBIORÓW DANYCH OSOBOWYCH ORAZ PROGRAMY ZASTOSOWANE DO PRZETWARZANIA TYCH DANYCH

§ 1

Wykaz zbiorów danych osobowych oraz metod zastosowanych do przetwarzania tych danych zawiera załącznik nr 2 do Polityki Bezpieczeństwa.

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

§1

Rejestr czynności przetwarzania danych osobowych zawierający opis struktury zbiorów danych osobowych (wskazanych z załączniku nr 2 do Polityki Bezpieczeństwa) zawiera załącznik nr 3.

PRZECHOWYWANIE DANYCH OSOBOWYCH W FORMIE PAPIEROWEJ

§1

Dane w postaci papierowej przetwarzane są w zakresie i na zasadach określonych w niniejszej Polityce Bezpieczeństwa.

§2

1. Dane archiwalne w postaci papierowej przechowywane są w wyznaczonych miejscach takich jak zamykane szafy
2. Dostęp do danych archiwalnych w postaci tradycyjnej (papierowej) posiadają jedynie osoby upoważnione pisemnie przez AD lub IDO.
3. Dane w postaci papierowej wykorzystywane do pracy bieżącej po zakończeniu pracy przechowywane są w zamkniętych szafach kartotecznych lub innych zamkniętych szafach meblowych.
4. Możliwe jest pozostawianie dokumentacji w postaci papierowej w otwartych szafach i regałach meblowych w przypadku gdy pomieszczenia, w których znajdują się szafy/ regały są zabezpieczone przed dostępem osób niepowołanych, jednakże dokumentacja ta powinna zostać zabezpieczona/schowana do zamykanej szafy przed końcem pracy osoby pracującej na te dokumentacji.
5. Dostęp do pomieszczeń, gdzie przechowywane są dane osobowe mają jedynie osoby upoważnione.

STRATEGIA ZABEZPIECZENIA DANYCH OSOBOWYCH, DZIAŁANIA NIEZBĘDNE DO ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETAWARZANYCH DANYCH OSOBOWYCH

§1

Celem wprowadzonych niniejszą Polityką zabezpieczeń i obostrzeń jest ochrona danych osobowych.

§2

System informatyczny Administratora Danych posiada połączenie z Internetem (sieć publiczna), w związku z czym niniejszy dokument służy zapewnieniu odpowiedniego do zagrożeń poziomu zabezpieczeń danych osobowych już na etapie ich pozyskiwania/zbierania Do realizacji tego calu należy wykorzystać stosowane w organizacji zabezpieczenia systemów informatycznych oraz stosowane procedury opisane w niniejszym tytule Polityki Bezpieczeństwa.

§ 3

Bezpieczeństwo teleinformatyczne zapewnia się przez:
1. Ochronę fizyczną.
2. Ochronę elektromagnetyczną.
3. Ochronę kryptograficzną.
4. Bezpieczeństwo teletransmisji.
5. Kontrolę dostępu do urządzeń systemu lub sieci teleinformatycznej.
   Może również zostać zastosowana:
6. Pseudonimizacja

Po wprowadzeniu certyfikacji przez przepisy prawa, ASAP może starać się certyfikację swoich systemów zabezpieczających co jest równoznaczne ze spełnieniem wymogu RODO adekwatnego zabezpieczenia danych osobowych.

§4

Ochronę fizyczną systemu lub sieci teleinformatycznej zapewnia się przez instalację środków zabezpieczających pomieszczenia, w którym znajdują się urządzenia systemu lub sieci teleinformatycznej, w szczególności przed:
1. Nieuprawnionym dostępem.
2. Podglądem.

§5

Ochrona elektromagnetyczna polega na stosowaniu się do następujących zasad:
1. Wszelkie urządzenia systemu i sieci teleinformatycznej winny znajdować się w odległości nie mniejszej niż 150 m od źródeł emisji elektromagnetycznej mogącej zakłócać prawidłową pracę tych urządzeń.
2. W trakcie pracy urządzeń systemu i sieci teleinformatycznej w strefie bezpieczeństwa należy

wyłączyć urządzenia o wysokiej emisyjności fal elektromagnetycznych lub stosować urządzeń, połączeń linii o obniżonym poziomie emisji lub ich ekranowanie i filtrowanie zewnętrznych linii zasilających lub sygnałowych.

§6

1. Ochrona kryptograficzna systemu lub sieci teleinformatycznej polega na stosowaniu metod i środków zabezpieczających dane osobowe przez ich szyfrowanie oraz stosowanie innych mechanizmów kryptograficznych gwarantujących integralność i zabezpieczenie przed nieuprawnionym ujawnieniem tych danych.
2. Pseudonimizacja może być stosowana poprzez jedną z metod:
   a) szyfrowanie kluczem tajnym - obecność klucza pozwala jednocześnie utajnić zbiór danych i w razie konieczności ponownie go odczytać, przypisując konkretne informacje do konkretnych osób. W domyśle jedynie posiadanie klucza daje możliwość odszyfrowania danych;
   b) tokenizacja - jest to technika szyfrowania jednokierunkowego i polega na zastąpieniu fragmentów danych ciągiem losowych liczb, co sprawia, że informacje te stają się bezużyteczne dla osób postronnych. Metoda ta często jest wykorzystywana w branży finansowej;
   c) skracanie - czyli skrócenie wybranych wartości, tak aby odczytanie ich faktycznego znaczenia stało się niemożliwe.

§7

Określone sposoby zabezpieczeń dotyczą:

1. Zabezpieczeń przed dostępem do danych osób nieupoważnionych na etapie eksploatacji systemu tj. wprowadzanie danych, aktualizacji lub usuwania danych, wyświetlania lub dokonywania zestawień, wypisów.
2. Ochrony danych zarchiwizowanych na nośnikach zewnętrznych, procedur niszczenia niepotrzebnych wydruków lub nośników danych.
3. Systemu zabezpieczeń przed dostępem osób niepowołanych do pomieszczeń, w których są eksploatowane urządzenia oraz sposobów dostępu do tych pomieszczeń pracowników, personelu pomocniczego oraz serwisu zewnętrznego.
4. Monitorowania systemu zabezpieczeń.
5. Zakresu obowiązków pracowników w części dotyczącej bezpieczeństwa danych.

§8

Strategia ochrony danych osobowych opiera się na następujących zasadach:

1. Fizyczny dostęp do pomieszczeń, w których eksploatowane są systemy informatyczne blokują drzwi zamykane na zamki mechaniczne lub elektromagnetyczne.

2. Dostęp do budynków, w których przetwarzane są dane osobowe jest monitorowany lub ewidencjonowany przez służbę ochrony lub zewnętrzną firmę ochroniarską.
3. Dostęp do pomieszczeń, w których przetwarzane są dane osobowe posiadają jedynie uprawnieni pracownicy.
4. Podstawowym sposobem zabezpieczenia danych przetwarzanych w systemach informatycznych jest system definiowania użytkowników, grup użytkowników oraz haseł. Są to zabezpieczenia programowe wmontowane w eksploatowane systemy uniemożliwiające dostęp do systemu osobom nieupoważnionym,
5. Dodatkowym systemem zabezpieczenia jest stosowanie kryptograficznej ochrony danych, jaką oferuje wykorzystywane oprogramowanie. Ochrona kryptograficzna systemu lub sieci teleinformatycznej polega na stosowaniu metod i środków zabezpieczających dane osobowe przez ich szyfrowanie oraz stosowanie innych mechanizmów kryptograficznych gwarantujących integralność i zabezpieczenie przed nieuprawnionym ujawnieniem tych danych takich jak np. pseudonimizacja.

§9

Należy chronić dokumenty papierowe zawierające dane osobowe przed ich fizycznym uszkodzeniem lub zniszczeniem, w szczególności:

1. Dokumenty papierowe zawierające dane osobowe muszą być chronione przed zagrożeniami ze strony otoczenia (ogień, wyciek wody itp.).
2. Dokumenty papierowe powinny być fizycznie chronione przed kradzieżą, zniszczeniem lub niewłaściwym używaniem. Opuszczając stanowisko pracy należy sprawdzić czy są one zamknięte w odpowiednich szafach.
3. Usunięcie lub wyniesienie poza komórki organizacyjne ASAP dokumentu papierowego zawierającego dane osobowe, wymaga zachowania szczególnej ostrożności i możliwe jest tylko i wyłącznie w czasie pełnienia obowiązków służbowych wynikających z charakteru pracy. Wynoszony dokument powinien zawierać minimum informacji tzn. tylko informacje konieczne do wykonania określonego zadania.
4. Utrata i kradzież dokumentów papierowych zawierających dane osobowe powinna być niezwłocznie zgłoszona bezpośredniemu przełożonemu.
5. Każdy dokument papierowy zawierający dane osobowe, mający charakter dokumentu roboczego, należy na koniec pracy zniszczyć w niszczarce papieru lub schować w odpowiedniej zamykanej szafie/szufladzie.

§10

1. Nośniki magnetyczne (płyty, pendrive, dyskietki, itp.) zawierające dane osobowe należy bezwzględnie zabezpieczyć przed ich kradzieżą, fizycznym uszkodzeniem lub zniszczeniem, co uniemożliwiłoby odczytanie lub odzyskanie informacji w nich zawartych.
2. Nośniki magnetyczne i optyczne zawierające dane osobowe należy bezwzględnie chronić przed zagrożeniami ze strony otoczenia (kurz, promieniowanie elektromagnetyczne, ogień, wyciek wody itp.).
3. Opuszczając stanowisko pracy należy sprawdzić czy są one zamknięte w odpowiednich szafach.
4. Wszystkie nośniki magnetyczne i optyczne zawierające dane osobowe muszą być oznaczone dla ich identyfikacji.
5. Zabrania się kopiowania jakichkolwiek zbiorów danych osobowych z nośników magnetycznych i optycznych bez zgody osób upoważnionych do reprezentowania Administratora Danych.
6. Zabrania się kopiowania jakichkolwiek dokumentów zawierających dane osobowe poprzez wykonanie zdjęcia aparatem fotograficznym/telefonem.
7. Nośniki magnetyczne i optyczne zawierające dane osobowe nie mogą być wynoszone poza siedzibę ASAP jeżeli ich wyniesienie nie ma związku z wykonywaniem obowiązków służbowych i jest niezbędne do ich wykonania.
8. Dyski magnetyczne i optyczne zawierające dane osobowe mogą być wynoszone poza teren ASAP (np. dyskietki, czy CD-ROM, DVD i inne) przez osoby upoważnione do przetwarzania danych osobowych.
9. Dyski twarde lub inne nośniki magnetyczne i optyczne zawierające dane osobowe, przeznaczone do przekazania imieniu podmiotowi, nieuprawnionemu do otrzymania danych osobowych, pozbawia się wcześniej zapisu tych danych.
10. Dyski twarde komputerów przeznaczone do naprawy, a zawierające dane osobowe, pozbawia się przed naprawą zapisu tych danych w sposób uniemożliwiający ich odtworzenie albo naprawia się je pod nadzorem osoby upoważnionej przez Administratora Danych
11. Niszczenia zużytych lub uszkodzonych nośników magnetycznych i optycznych zawierających dane osobowe dokonuje się za zgodą Inspektora Danych Osobowych.
12. Niszczenie zużytych lub uszkodzonych nośników magnetycznych i optycznych zawierających dane osobowe dokonuje się wg. zasad:
    a) Płyty CD/DVD - należy zniszczyć w niszczarce dokumentów.
    b) Twarde dyski - rozmontować urządzenie w celu odsłonięcia talerzy z zapisem magnetycznym, a następnie używając twardego i ostrego narzędzia zniszczyć powierzchnię dysku poprzez zarysowanie jej kilkudziesięcioma rysami, lub należy użyć młotka w celu zniszczenia talerzy magnetycznych i ceramicznych.
    c) Pendrive - należy użyć młotka w celu uszkodzenia układów pamięci poprzez ich fizyczne zniszczenie.

13. Utrata lub kradzież nośnika magnetycznego i optycznego z danymi osobowymi powinna być niezwłocznie zgłoszona bezpośredniemu przełożonemu.

§11

Wprowadza się następujące zabezpieczenia danych osobowych przetwarzanych w systemie informatycznym:

1. Zalogowanie się do programu wymaga podania nazwy użytkownika i hasła. Każdy użytkownik ma przypisane uprawnienia do wykonywania operacji.
2. Oprogramowanie wykorzystywane do przetwarzania danych posiada własny system i uprawnień kont (zabezpieczonych hasłami).
3. Administrator Systemu Informatycznego lub inna osoba upoważniona przez Administratora Danych ma uprawnienia do definiowania identyfikatorów użytkowników i haseł.
4. Wykorzystany jest system szyfrowania danych (dostępny w systemie operacyjnym) uniemożliwiający odczyt danych osobom nieupoważnionym.
5. W celu ochrony przed dostępem do danych komputera z sieci publicznej wykorzystuje się system zapory ogniowej dostępnej w systemie operacyjnym.
6. Stosuje się aktywną ochronę antywirusową w czasie rzeczywistym na każdym komputerze, na którym przetwarzane są dane osobowe.
7. Kopie zapasowe na nośnikach przenośnych wykonuje osoba upoważniona przez Administratora Danych.
8. Kopie bezpieczeństwa przechowywane są pod nadzorem osoby upoważnionej przez Administratora Danych.
9. Dostęp do nośników zawierających kopie danych mają tylko uprawnione osoby.

§ 12

Stosuje się następujące zabezpieczenia organizacyjne przed dostępem do danych osób niepowołanych:

1. Dostęp do danych mają wyłącznie pracownicy upoważnieni do przetwarzania danych osobowych.
2. W pokojach/gabinetach, do których dostęp mają petenci monitory komputerowe ustawione są w ten sposób, by petenci nie widzieli zapisów na ekranie.
3. W przypadku dłuższej bezczynności uruchamiane są tzw. wygaszacie ekranu, których dezaktywacja jest możliwa po podaniu prawidłowego hasła użytkownika.

§ 13

Ryzyko utraty bezpieczeństwa przetwarzanych przez Administratora Danych i osób, które mają dostęp do danych osobowych (np. ryzyko utraty bezpieczeństwa danych pojawiające się ze strony osób trzecich, serwisanci, podmiot przetwarzający), jest minimalizowane przez zawieranie umów powierzenia przetwarzania danych osobowych.

§14

Ryzyko ze strony osób, które potencjalnie mogą w łatwiejszy sposób uzyskać dostęp do danych osobowych (np. osoby sprzątające pomieszczenia ASAP), jest minimalizowane przez zobowiązywanie ich do zachowania tajemnicy na podstawie odrębnych, pisemnych oświadczeń lub na podstawie odpowiednich zapisów w umowach.

§15

Ryzyko utraty bezpieczeństwa danych przetwarzanych przez Administratora Danych na serwerach zewnętrznych (hosting) lub przy współpracy z przetwarzającym jest minimalizowane przez zawieranie umów powierzenia przetwarzania danych osobowych.

§16

Treść umowy powierzenia przetwarzania danych osobowych powinna zostać sporządzona indywidualnie, dla konkretnego przypadku przetwarzania danych, w sposób uwzględniający wszystkie elementy gwarantujące prawidłowe zabezpieczenie i przetwarzanie danych osobowych zgodnie z RODO oraz zawierać co najmniej:

1. przedmiot przetwarzania,
2. czas trwania przetwarzania,
3. charakter i cel przetwarzania,
4. rodzaj danych osobowych,
5. kategorię osób, których dane dotyczą,
6. obowiązki i prawa administratora,
7. obowiązki podmiotu przetwarzającego.
8. wskazanie szczegółowego zakresu w jakim powierzane dane mogą być przetwarzane,
9. wskazanie sposobu zwrotu powierzonych danych i/lub sposobu w jakim powierzone dane zostaną usunięte po zakończeniu umowy,
10. uprawnienie do kontroli podmiotu przetwarzającego w zakresie zgodności jego działalności z przepisami RODO i obowiązującymi wymogami w zakresie ochrony praw osób, których dane są przetwarzane.

§17

Dla zachowania bezpieczeństwa danych zobowiązuje się osoby upoważnione do:

1. ustawiania ekranów komputerowych tak, by osoby niepowołane nie mogły oglądać ich zawartości, a zwłaszcza nie naprzeciwko wejścia do pomieszczenia lub w „otwartej" rejestracji.
2. Niepozostawiania bez kontroli dokumentów, nośników danych i sprzętu.

3. Niepodłączania do listew podtrzymujących napięcie przeznaczonych dla sprzętu komputerowego innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejniki, czajniki, wentylatory).
4. Nieużywania powtórnie dokumentów zadrukowanych jednostronnie.
5. Niezapisywania hasła wymaganego do uwierzytelnienia się w systemie na papierze lub innym niezabezpieczonym nośniku.
6. Powstrzymywania się przez osoby upoważnione do przetwarzania danych osobowych od samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu (szczególnie komputerów przenośnych), nawet gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych.
7. Przestrzegania przez osoby upoważnione do przetwarzania danych osobowych swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowana się do zaleceń obowiązujących u Administratora Danych.
8. Opuszczania stanowiska pracy dopiero po aktywizowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w sposób uniemożliwiający podgląd danych.
9. Nie wynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich wypisów, nawet w postaci zaszyfrowanej.
10. Niszczenia w sposób uniemożliwiający odczytanie lub chowania do szaf zamykanych na klucz wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy i po zakończeniu dnia pracy.
11. Niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych.
12. Chowania do zamykanych na klucz szaf wszelkich akt zawierających dane osobowe przed opuszczeniem miejsca pracy w tym po zakończeniu dnia pracy.
13. Umieszczania kluczy do szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy.
14. Zamykania okien w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych.
15. Zamykania okien w razie opuszczania pomieszczenia, w tym po zakończeniu dnia pracy.
16. Zamykania/blokowania drzwi po zakończeniu pracy w danym dniu.

§18

Zobowiązuje się osoby upoważnione do przetwarzania danych osobowych do stosowania następujących zasad:

1. Przestrzeganie innych wymogów bezpieczeństwa systemowego określonych w instrukcjach obsługi producentów sprzętu i używanych programach.
2. Przed atakami z sieci zewnętrznej wszystkie komputery (w tym także przenośne) chronione są środkami dobranymi przez Administratora Danych.

3. Administrator Danych dobiera elektroniczne środki ochrony przed atakami z sieci stosownie do pojawiania się nowych zagrożeń, a także stosownie do rozbudowy systemu informatycznego Administratora Danych i powiększania bazy danych.

§19

1. Poszczególnym osobom upoważnionym do przetwarzania danych osobowych przydziela się konta opatrzone niepowtarzalnym identyfikatorem, umożliwiające dostęp do danych, zgodnie z zakresem upoważnienia do ich przetwarzania.
2. Tryb nadawania identyfikatorowi haseł określa Instrukcja Zarządzania Systemami Informatycznymi stanowiąca załącznik nr 4.

§20

Prezes lub IDO w sytuacji jego wyznaczenia, zleca i nadzoruje wykonanie przeglądu przetwarzanych danych osobowych pod kątem celowości ich dalszego przetwarzania. Osoby upoważnione do przetwarzania danych osobowych, są obowiązani wskazywać te dane osobowe, które powinny zostać usunięte ze względu na zrealizowanie celu przetwarzania danych osobowych lub brak ich adekwatności do realizowanego celu. Przeglądu przetwarzanych danych osobowych pod kątem celowości ich dalszego przetwarzania przeprowadzany jest co najmniej raz w roku lub w razie potrzeby.

§21

1. Udostępnianie danych osobowych funkcjonariuszom Policji może nastąpić tylko po przedłożeniu wniosku o przekazanie lub udostępnienie informacji. Wniosek ten powinien mieć formę pisemną i zawierać:
   a) oznaczenie wnioskodawcy,
   b) wskazanie przepisów uprawniających do dostępu do informacji,
   c) określenie zakresu potrzebnych informacji oraz formy ich przekazania lub udostępnienia.
   d) wskazanie imienia, nazwiska i stopnia służbowego policjanta upoważnionego do pobrania informacji lub zapoznania się z ich treścią.
2. Udostępnianie danych osobowych na podstawie ustnego wniosku zawierającego wszystkie powyższe cztery elementy wniosku pisemnego może nastąpić tylko wtedy, gdy zachodzi konieczność niezwłocznego działania, np. w trakcie pościgu za osobą podejrzaną o popełnienie czynu zabronionego albo podczas wykonywania czynności mających na celu ratowanie życia i zdrowia ludzkiego lub mienia.
3. Osoba udostępniająca dane osobowe jest obowiązana zażądać od policjanta pokwitowania pobrania dokumentów zawierających informacje przekazane na podstawie pisemnego wniosku albo

potwierdzenia faktu uzyskania wglądu w treść informacji. Policjant jest obowiązany do pokwitowania lub potwierdzenia.

4. Jeśli informacje są przekazywane na podstawie ustnego wniosku, należy stosownie do okoliczności zwrócić się z prośbą i pokwitowanie albo potwierdzenie. Jeśli pokwitowanie albo potwierdzenie ze względu na okoliczności udostępniania nie są możliwe, osoba udostępniająca informacje sporządza na tę okoliczność notatkę służbową.
5. Osoba upoważniona może udostępnić dane osobowe innym służbom, podmiotom lub osobom fizycznym ustawowym do ich otrzymania na mocy obowiązujących przepisów prawa (np., komornikom).

§23

1. Niezastosowanie się do prowadzonej przez Administratora Danych Polityki Bezpieczeństwa Informacji przetwarzania danych osobowych, której założenia określa niniejszy dokument i naruszenie procedur ochrony danych przez pracowników i upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie podstawowych obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia z winy pracownika na podstawie art. 52 Kodeksu pracy.
2. Niezależnie od rozwiązania stosunku pracy osoby naruszające zasady przetwarzania danych mogą zostać pociągnięte do odpowiedzialności karnej na podstawie art. 266 Kodeksu karnego.

§24

1. AD uwzględnia następujący plan szkoleń prowadzonych przez IDO lub inną wyznaczoną osobę:
   a) Szkolenie każdej nowo zatrudnionej osoby, która ma być upoważniona do przetwarzania danych osobowych w systemach informatycznych funkcjonujących w ASAP.
   b) Szkolenia wewnętrzne wszystkich osób upoważnionych do przetwarzania danych osobowych przeprowadzane są w przypadku każdej zmiany zasad lub procedur ochrony danych osobowych w systemach informatycznych funkcjonujących w ASAP.
2. System szkoleń obejmuje pracowników zatrudnionych bezpośrednio przy przetwarzaniu danych, w tym danych osobowych.
3. Tematyka szkoleń obejmuje:

a) Przepisy i procedury ochrony danych osobowych, sporządzania i przechowywania ich kopii, niszczenia wydruków i zapisów, na nośnikach.
b) Sposoby ochrony danych osobowych przed osobami postronnymi i procedury udostępniania danych osobom, których one dotyczą,
c) Obowiązki osób upoważnionych do przetwarzania danych osobowych.
d) Odpowiedzialność za naruszenie obowiązków z zakresu ochrony danych osobowych.
e) Zasady i procedury określone w Polityce Bezpieczeństwa.

4. Bezpośredni przełożony lub IDO jeśli jest powołany, zapoznaje każdą nowo zatrudnioną osobę, która ma być upoważniona do przetwarzania danych osobowych, z zapisami niniejszego dokumentu, procedurami bezpieczeństwa informacji oraz zapisami RODO.

ŚRODKI TECHNICZNE I ORGANIZACYJNE SŁUŻĄCE ZAPEWNIENIU POUFNOŚCI, INTEGRALNOŚCI, RZETELNOŚIC I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH OSOBOWYCH STOSOWANE W ASAP

§1

1. Zabezpieczenia organizacyjne:
   a) Sporządzono i wdrożono Politykę Bezpieczeństwa.
   b) Sporządzono i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
   c) Do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez Administratora danych bądź osobę przez mego upoważnioną.
   d) Stworzono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych.
   e) Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego.
   f) Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy.
   g) Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych.
   h) Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych.
   i) Dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonując takiej ich modyfikacji, która nie pozwoli na odtworzenie treści, aby po dokonaniu usunięcia danych niemożliwa była identyfikacja osób.
2. Zabezpieczenia techniczne:
   a) Stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową.
   b) Komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, pomocą indywidualnego identyfikatora użytkowania.
   c) Wygaszacze ekranu
   d) Okresowe wymuszanie zmiany hasła
3. Środki ochrony fizycznej:

a) Obszar, na którym przetwarzane są dane osobowe, poza godzinami pracy, chroniony jest alarmem.
b) Budynki w których przetwarzane i przechowywane są dane osobowe ochraniane są przez firmę zewnętrzną.
c) Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi).
d) Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności na włamanie - drzwi klasy C.
e) Zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej.
f) Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy.
g) Dostęp do pomieszczeń, w których przetwarzany jest zbiory danych osobowych objęte są systemem kontroli dostępu.
h) Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych.
i) Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętym sejfie lub kasie pancernej.
j) Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego lub wolnostojącej gaśnicy.

§3

1. Najwyższe uprawnienia w systemie informatycznym posiada Prezes Zarządu lub osoba przez niego upoważniona lub Administrator Systemów Informatycznych (ASI).
2. ASI lub ewentualnie inna osoba upoważniona przez Prezesa Zarządu jest osobą uprawnioną do instalowania i usuwania oprogramowania systemowego i narzędziowego.
3. Dopuszcza się instalowanie tylko legalnie pozyskanych programów, niezbędnych wykonywania zadań ASAP i posiadających ważną licencję użytkowania.

§4

1. Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych, może uzyskać wyłącznie osoba (użytkownik) zarejestrowana w tym systemie.
2. Dostęp do systemów operacyjnych, serwerów, stacji roboczych powinien być chroniony przez nazwę użytkownika i hasło.
3. Identyfikator użytkownika składa się z ciągu znaków literowych. W identyfikatorze pomija się polskie znaki diakrytyczne.

4. Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne. Hasła zmienia się nie rzadziej niż co 30 dni.
5. Hasła w systemie informatycznym powinny być przechowywane w postaci zaszyfrowanej.
6. Pierwsze hasło jest przekazywane użytkownikowi ustnie.
7. Użytkownikom systemu nie wolno udostępniać swojego identyfikatora i hasła innym osobom.

§5

Należy rygorystycznie przestrzegać wymogu przechowywania nośników zawierających awaryjne kopie danych i systemów w pomieszczeniach innych niż pomieszczenia, w których przechowywane są dane przeznaczone do bieżącego użytku. Jednocześnie dane te muszą być odpowiednio zabezpieczone fizycznie oraz zaszyfrowane.

§6

1. Wszystkie stacje robocze, muszą być chronione programem antywirusowym, sprawdzającym w trybie rzeczywistym wszystkie przychodzące i wychodzące pliki.
2. Zabronione jest blokowanie pracy programu antywirusowego.
3. Dla zapewnienia ochrony przed wirusami i innymi niepożądanymi kodami sprawdza się wszystkie zbiory przychodzące z sieci i Internetu.

§7

W związku z dynamicznym rozwojem technik służących do atakowania systemów informatycznych Prezes Zarządu powinien na bieżąco śledzić informacje na temat wykrytych luk i wprowadzać zalecane zabezpieczenia.

§8

1. System ochrony powinien być w sposób ciągły nadzorowany i możliwie często aktualizowany.
2. Kontrole i testy powinny obejmować zarówno dostęp do zasobów systemu, jak i profile oraz uprawnienia poszczególnych użytkowników.

§9

1. Wszelkie naprawy i konserwacje sprzętu i oprogramowania mogą odbywać się tylko w obecności osób uprawnionych.
2. Urządzenia informatyczne służące do przetwarzania danych osobowych można przekazać do naprawy dopiero po uzyskaniu zgody Prezesa Zarządu lub osoby przez niego upoważnionej.

OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

§1

Zagrożenia naruszające ochronę danych osobowych są następujące:

1. Zagrożenia których występowanie może prowadzić do utraty integralności danych ich zniszczenia lub uszkodzenia infrastruktury technicznej systemu.
2. Zagrożenia zamierzone, świadome i celowe naruszenia poufności danych, (bez uszkodzenia infrastruktury technicznej i zakłócenia ciągłości pracy).

§2

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to w szczególności:

1. Sytuacje losowe lub nieprzewidziane oddziaływanie na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń itp.
2. Awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a tym sam fakt pozostawienia serwisantów bez nadzoru.
3. Pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu.
4. Stwierdzenie próby lub modyfikacji danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji).

§3

Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsca przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, w formie niezabezpieczonej itp.

ZASADY POSTĘPOWANIA W SYTUACJI NARUSZENIA SYSTEMU OCHRONY DANYCH OSOBOWYCH

§1

1. Naruszeniem zabezpieczenia danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom

nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia lub usunięcia, a w szczególności:

a) nieautoryzowany dostęp do danych,
b) nieautoryzowane modyfikacje lub zniszczenie danych,
c) udostępnienie danych nieautoryzowanym podmiotom,
d) nielegalne ujawnienie danych,
e) pozyskiwanie danych z nielegalnych źródeł.

2. W przypadku stwierdzenia naruszenia zabezpieczeń lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik zatrudniony przy przetwarzaniu danych osobowych jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie zgłosić fakt naruszenia Prezesowi lub Inspektorowi Danych Osobowych, a następnie postępować stosownie do podjętej przez niego decyzji.
3. Zgłoszenie naruszenia zabezpieczeń danych osobowych powinno zostać sporządzone zgodnie z Załącznikiem nr 5 i zawierać:
   a) opisanie symptomów naruszenia zabezpieczeń danych osobowych,
   b) określenie sytuacji i czasu w jakim stwierdzono naruszenie zabezpieczeń danych osobowych,
   c) określenie wszelkich istotnych informacji mogących wskazywać na przyczynę naruszenia,
   d) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.
4. AD lub Inspektor Danych Osobowych, jeśli jest powołany lub inna upoważniona osoba podejmuje wszelkie działania mające na celu:
   a) minimalizację negatywnych skutków zdarzenia,
   b) wyjaśnienie okoliczności zdarzenia,
   c) zabezpieczenie dowodów zdarzenia,
   d) umożliwienie dalszego bezpiecznego przetwarzania danych.
5. W celu realizacji procedury opisanej w niniejszym tytule AD lub Inspektor Danych Osobowych lub inna upoważniona przez niego osoba ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, a w szczególności:
   a) żądania wyjaśnień od pracowników,
   b) korzystania z pomocy konsultantów,
   c) nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.
6. Inspektor Danych Osobowych po zażegnaniu sytuacji naruszającej bezpieczeństwo danych osobowych opracowuje raport końcowy, w którym przedstawia przyczyny i skutki zdarzenia oraz wnioski, w tym kadrowe, ograniczające możliwość wystąpienia zdarzenia w przyszłości. Wzór raportu stanowi Załącznik nr 6 do niniejszej Polityki Bezpieczeństwa.
7. W przypadku naruszenia ochrony danych osobowych w organizacji, administrator danych bez zbędnej zwłoki, w terminie 72 godzin po stwierdzeniu naruszenia, będzie zobowiązany zgłosić takie naruszenie organowi nadzorczemu, tj. GIODO/Prezesowi Urzędu Ochrony Danych Osobowych,

chyba że jest mało prawdopodobne, by takie naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

8. Polecenia Inspektora lub innej upoważnionej przez niego osoby wydawane w celu realizacji zadań wynikających z niniejszej instrukcji są priorytetowe i powinny być wykonywane przed innymi poleceniami, zapewniając ochronę danych osobowych.
9. Odmowa udzielenia wyjaśnień lub współpracy z Inspektorem Danych Osobowych lub inną upoważnioną przez niego osobą traktowana będzie jako naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności cywilnoprawnej lub odpowiedzialności dyscyplinarnej określonej w Kodeksie Pracy.

POSTANOWIENIA KOŃCOWE

§1

AD lub Inspektor Danych Osobowych prowadzi ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie podstawowych obowiązków pracowniczych. Nałożona kara dyscyplinarna, nie wyklucza odpowiedzialności karnej tej osoby zgodnie z Ustawą.

LISTA ZAŁĄCZNIKÓW

Załącznik 1. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.

Załącznik 2. Szczegółowy wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do ich przetwarzania

Załącznik 3. Rejestr czynności przetwarzania danych osobowych

Załącznik 4. Ewidencja osób upoważnionych do przetwarzania danych osobowych

Załącznik 5. Upoważnienie do przetwarzania danych osobowych wraz z oświadczeniem o zachowaniu poufności

Załącznik 6. Instrukcja określająca sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Załącznik 7.Wzory klauzul realizujących obowiązek informacyjny ADO

ZAŁĄCZNIK 1

WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE			
LP.	**MIEJSCE PRZETWARZANIA DANYCH OSOBOWYCH**	**ADRES**	**ZABEZPIECZENIA POMIESZCZENIA / KONTROLA DOSTĘPU**
1.	główne miejsce prowadzenia działalności - siedziba	ul. Komitet Obrony Robotników 72, 02-146 Warszawa	Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych przez cała dobę jest nadzorowany przez służbę ochrony. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych jest w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez

			system monitoringu z zastosowaniem kamer przemysłowych. Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej niemetalowej szafie. Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej metalowej szafie.
2.	zakład produkcyjny	Raszyn, Al. Krakowska 48 A.	j.w.
3.	Komputery przenośne (laptopy), komputery stacjonarne, routery, smartfony, serwery	ul. Komitet Obrony Robotników 72, 02-146 Warszawa	Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła. Zbiór danych osobowych przetwarzany jest przy użyciu komputera przenośnego Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła. Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity. Użyto system Firewall do ochrony dostępu do sieci komputerowej Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

ZAŁĄCZNIK 2. SZCZEGÓŁOWY WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO ICH PRZETWARZANIA

W ASAP przetwarzane są następujące zbiory danych osobowych:

Lp.	**Nazwa i Opis Zbioru**	**Stosowane programy**
1.	Pracownicy i ich rodziny	Adobe Reader, Microsoft Office,
2.	Stażyści	Adobe Reader, Microsoft Office,
3.	Kontrahenci	Adobe Reader, Microsoft Office, Poligraf,
4.	Klienci	Adobe Reader, Microsoft Office, Poligraf,

ZAŁĄCZNIK 3. REJESTR PRZETWARZANIA DANYCH OSOBOWYCH.

Rejestr czynności przetwarzania prowadzony przez ADO

		DANE KONTAKTOWE
NAZWA ADMINISTRATORA	ASAP Polska sp. z o.o.	ul. Komitet Obrony Robotników 72, 02-146 Warszawa
NAZWY WSPÓŁADMINISTRATORÓW		
NAZWA PRZEDSTAWICIELA		
IMIĘ I NAZWISKO INSPEKTORA		

Kategorie osób, których dane dotyczą	Kategorie danych osobowych	Kategorie odbiorców, którym dane ujawniono lub zostaną ujawnione	Nazwa państwa trzeciego, do którego dane są przekazywane	Planowane terminy usunięcia danych	Cel przetwarzania
pracownicy i członkowie ich rodzin	Imiona i nazwiska, imiona rodziców, adres zamieszkania, adres zameldowania, PESEL, NIP, wykształcenie, seria i nr dowodu osobistego, nr telefonu, adres email, nr rachunku bankowego, stan rodzinny, data i miejsce urodzenia, obywatelstwo, przebieg dotychczasowego zatrudnienia, nr książeczki wojskowej, dane dot. urzędu skarbowego, dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w	Biuro rachunkowe, ZUS, US,	nie	zgodnie z art. 94 pkt 9a Kodeksu pracy obowiązkiem pracodawcy jest przechowywanie akt osobowych i dokumentacji płacowej. Aktualnie dokumenty te powinny być przechowywane przez cały okres zatrudnienia pracownika oraz przez kolejne 50 lat od zakończenia pracy u danego pracodawcy.	zawarcia i wykonania umowy oraz wykonania ciążących na ASAP obowiązków prawnych – księgowych

	postępowaniu sądowym lub administracyjnym				
Kontrahenci	Imiona i nazwiska, miejsce pracy, stanowisko, nr telefonu, adres email, regon, nip, adres firmy	Biuro rachunkowe, InCubi sp. z o.o.	nie	5 lat od rozwiązania umowy z uwagi na brzmienie art. 74 ust. 2 pkt 4 Ustawy o rachunkowości	zawarcia i wykonania umowy oraz wykonania ciążących na ASAP obowiązków prawnych – księgowych
Klienci	Imiona i nazwiska, miejsce pracy, stanowisko, nr telefonu, adres email, regon, nip, adres pracodawcy	Biuro rachunkowe, InCubi sp. z o.o.	nie	5 lat od rozwiązania umowy z uwagi na brzmienie art. 74 ust. 2 pkt 4 Ustawy o rachunkowości	zawarcia i wykonania umowy
Stażyści	Imiona i nazwiska, imiona rodziców, adres zamieszkania, adres zameldowania, PESEL, NIP, wykształcenie, seria i nr dowodu osobistego, nr telefonu, adres email, nr rachunku bankowego, stan rodzinny, data i miejsce urodzenia, obywatelstwo, przebieg dotychczasowego zatrudnienia, nr książeczki wojskowej, dane dot. urzędu skarbowego	biuro rachunkowe	nie	przez okres trwania stażu	realizacja umowy o praktyki/staż

ZAŁĄCZNIK 4. EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Ewidencja znajduje się w załączonym pliku MS Excel prowadzonym przez AD lub IDO

ZAŁĄCZNIK 5. UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH WRAZ Z OŚWIADCZENIEM O ZACHOWANIU POUFNOŚCI

UPOWAŻNIENIE

Upoważniam Panią/Pana [Imię i nazwisko] zatrudnioną/zatrudnionego na stanowisku

.....

do przetwarzania danych osobowych przetwarzanych w firmie ASAP Polska sp. z o.o. w związku z realizacją zadań wynikających z zawartej z Panią/Panem umowy o pracę/ umowy zlecenia. Jednocześnie zobowiązuję Panią/Pana do zachowania tych danych oraz sposobów ich zabezpieczenia w tajemnicy, zarówno w trakcie zatrudnienia jak i po ustaniu stosunku pracy/ zlecenia.

_____ _____

miejscowość, data podpis

OŚWIADCZENIE

Oświadczam, że znane mi są przepisy prawa oraz obowiązujące w ASAP Polska sp. z o.o. procedury postępowania w zakresie dotyczącym ochrony danych osobowych. Znane mi są również konsekwencje prawne oraz służbowe jakie ponosi osoba nie stosująca się do wymogów określonych we wspomnianych powyżej przepisach i procedurach.

Zobowiązuję się do przestrzegania przepisów prawa oraz obowiązujących w ASAP Polska sp. z o.o. procedur postępowania w zakresie dotyczącym ochrony danych osobowych, w szczególności do nie ujawniania danych osobowych, do których mam dostęp oraz nie ujawniania ich zabezpieczeń, w czasie zatrudnienia lub zaangażowania ASAP Polska sp. z o.o., jak również po ustaniu stosunku pracy (lub wykonaniu albo wygaśnięciu innej umowy, na podstawie której byłem zaangażowany do współpracy).

_____ _____

miejscowość, data podpis osoby składającej oświadczenie

ZAŁĄCZNIK 6. INSTRUKCJA OKREŚLAJĄCA SPOSÓB ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH.

Instrukcja znajduje się w osobnym pliku

ZAŁĄCZNIK 7. WZÓR KLAUZUL REALIZUJĄCYCH OBOWIĄZKI INFORMACYJNE ADO

Klauzula realizująca obowiązek informacyjny w stosunku do pracowników ASAP Polska sp. z o.o. (w przypadku, gdy dane zostały zebrane bezpośrednio od osoby, której dotyczą

„Informujemy, iż administratorem Twoich danych osobowych jest ASAP Polska sp. z o.o. ul. Komitetu Obrony Robotników 72, 02-146 Warszawa, KRS 0000582265, NIP 522-304-20-67

Inspektorem ochrony danych jest Pan/Pani (*imię i nazwisko inspektora) … (*e-mail lub inne dane kontaktowe) … (o ile powołany)
Pani/Pana dane osobowe przetwarzane będą w celu zawarcia i realizacji umowy o pracę a także w prawnie usprawiedliwionych celów Administratora Danych.

Przetwarzanie Pana/Pani danych jest niezbędne do wykonania umowy, której jest Pan/Pani stroną.

Odbiorcą Pani/Pana danych osobowych będą … (*można wymienić kategorię odbiorców o ile istnieją);

Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu.

Ma Pan/Pani prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.

Pana/Pani dane osobowe przechowywane będą przez okres 50 lat zgodnie z ustawa kodeks pracy.

Podanie przez Pana/Panią danych osobowych jest warunkiem zawarcia umowy). Jest Pan/Pani zobowiązana do ich podania a konsekwencją niepodania danych osobowych skutkować będzie nie zawarciem umowy o pracę.

Pani/Pana dane osobowe nie są przekazywane do krajów trzecich.

Klauzula realizująca obowiązek informacyjny w stosunku do kandydatów na pracowników w ASAP Polska sp. z o. o. (w przypadku, gdy dane zostały zebrane bezpośrednio od osoby, której dotyczą):

Informujemy, iż administratorem Twoich danych osobowych jest ASAP Polska sp. z o.o. ul. Komitetu Obrony Robotników 72, 02-146 Warszawa, KRS 0000582265, NIP 522-304-20-67

Pani/Pana dane osobowe przetwarzane są w celu przeprowadzeni rekrutacji na [•] stanowisko pracy oraz mogą zostać udostępnione (…). Posiada Pan/Pani prawo dostępu do treści swoich danych osobowych oraz ich poprawienia lub żądania ich usunięcia, a podanie ich treści jest dobrowolne.

Odbiorcą Pani/Pana danych osobowych będą … (*można wymienić kategorię odbiorców o ile istnieją);

Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania (jeżeli przetwarzanie odbywa się na podstawie zgody), którego dokonano na podstawie zgody przed jej cofnięciem;

Ma Pan/Pani prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.

Pana/Pani dane osobowe przechowywane będą przez okres rekrutacji po którym zostaną zniszczone.

Pani/Pana dane osobowe nie są przekazywane do krajów trzecich.

Klauzula realizująca obowiązek informacyjny w stosunku do kontrahentów ASAP Polska sp. z o.o. (w przypadku, gdy dane zostały zebrane bezpośrednio od osoby, której dotyczą):

Informujemy, iż administratorem Twoich danych osobowych jest ASAP Polska sp. z o.o. ul. Komitetu Obrony Robotników 72, 02-146 Warszawa, KRS 0000582265, NIP 522-304-20-67

Inspektorem ochrony danych jest Pan/Pani (*imię i nazwisko inspektora) … (*e-mail lub inne dane kontaktowe) … (o ile powołany)

Pani/Pana dane osobowe przetwarzane są w celu realizacji umowy oraz mogą zostać udostępnione firmie (…)

Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania (jeżeli przetwarzanie odbywa się na podstawie zgody), którego dokonano na podstawie zgody przed jej cofnięciem;

Pani/Pana dane osobowe przechowywane będą przez okres 5 lat zgodnie z ustawą o rachunkowości.

Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu.

Ma Pan/Pani prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.

Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego.

klauzula realizująca obowiązek informacyjny w stosunku do klientów w ASAP Polska sp. z o. o. (w przypadku, gdy dane zostały zebrane bezpośrednio od osoby, której dotyczą):

Informujemy, iż administratorem Twoich danych osobowych jest ASAP Polska sp. z o.o. ul. Komitetu Obrony Robotników 72, 02-146 Warszawa, KRS 0000582265, NIP 522-304-20-67
Inspektorem ochrony danych jest Pan/Pani (*imię i nazwisko inspektora) … (*e-mail lub inne dane kontaktowe) … (o ile powołany)

Pani/Pana dane osobowe przetwarzane są w celu realizacji zawartej z ASAP umowy oraz mogą zostać udostępnione firmie (…)

Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania (jeżeli przetwarzanie odbywa się na podstawie zgody), którego dokonano na podstawie zgody przed jej cofnięciem;

Pani/Pana dane osobowe przechowywane będą przez okres 5 lat zgodnie z ustawą o rachunkowości.

Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu.

Ma Pan/Pani prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.

Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego.

klauzula realizująca obowiązek informacyjny w stosunku do stażystów w ASAP Polska sp. z o. o. (w przypadku, gdy dane zostały zebrane bezpośrednio od osoby, której dotyczą):

Informujemy, iż administratorem Twoich danych osobowych jest ASAP Polska sp. z o.o. ul. Komitetu Obrony Robotników 72, 02-146 Warszawa, KRS 0000582265, NIP 522-304-20-67

Inspektorem ochrony danych jest Pan/Pani (*imię i nazwisko inspektora) … (*e-mail lub inne dane kontaktowe) … (o ile powołany)

Pani/Pana dane osobowe przetwarzane są w celu odbycia stażu oraz mogą zostać udostępnione firmie (…)

Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do

cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania (jeżeli przetwarzanie odbywa się na podstawie zgody), którego dokonano na podstawie zgody przed jej cofnięciem;

Pani/Pana dane osobowe przechowywane będą przez okres 50 lat zgodnie z kodeksem pracy

Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu.

Ma Pan/Pani prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.

Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego.