Polityka bezpieczeństwa

danych osobowych

HQS Systems spółka z ograniczoną odpowiedzialnością z siedzibą w Poznaniu

(zasady postępowania z danymi osobowymi

w działalności przedsiębiorcy)

Poznań , dnia 23 kwietnia 2025 r.

(wersja zaktualizowana)

…..……..

Podpis osoby reprezentującej
Administratora Danych Osobowych

Spis treści

ROZDZIAŁ I Ogólne zasady polityki bezpieczeństwa

1. Wprowadzenie

1.1. Polityka bezpieczeństwa jest wyrazem woli ADO w zakresie wdrożenia przepisów prawnych dotyczących ochrony danych osobowych.

1.2. Celem Polityki bezpieczeństwa jest określenie zasad ochrony danych osobowych oraz wskazanie działań jakie należy wykonać, aby właściwie zabezpieczać dane osobowe, a także utrzymywać zgodność operacji przetwarzania z przepisami w zakresie ochrony danych osobowych, w szczególności z 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 (dalej: „RODO")

1.3. Niniejsza Polityka została opracowana i wdrożona w oparciu o zapisy art. 24 ust. 2 RODO w celu zapewnienia organizacyjnych środków zabezpieczających przetwarzanie danych osobowych.

1.4. Polityka bezpieczeństwa obejmuje również swoim zakresem dane osobowe, które zostały powierzone przez inne podmioty.

1.5. Podstawy prawne w zakresie Polityki bezpieczeństwa danych osobowych stanowią:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dziennik Urzędowy UE L 119), dalej: RODO,
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jednolity Dz. U. 2018 r. poz. 1000 z późniejszymi zmianami), dalej: ustawa o ochronie danych osobowych,
- przepisy wykonawcze do ustawy o ochronie danych osobowych,
- Przepisy szczególne.

1.6. Polityka bezpieczeństwa dotyczy zadań związanych z zabezpieczeniem danych osobowych zarówno przetwarzanych w sposób tradycyjny (wersje papierowe), jak i w systemach informatycznych.

1.7. Jeżeli przepisy innych ustaw przewidują dalej idącą ochronę danych osobowych niż RODO lub ustawa o ochronie danych osobowych, stosuje się przepisy tych ustaw.

1.8. Bezpieczeństwo danych osobowych rozumiane jest jako zapewnienie poufności, integralności i dostępności. ADO dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były przetwarzane zgodnie z prawem, zbierane dla oznaczonych celów i nie poddawane przetwarzaniu niezgodnemu z tymi celami, adekwatne, stosowne, ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Ponadto, ADO zapewnia, aby przetwarzane dane były prawidłowe, przechowywane nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania oraz przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo.

1.9. Niniejsze zasady obowiązują wszystkich pracowników/współpracowników oraz osoby upoważnione do przetwarzania danych osobowych przez ADO. Wszyscy pracownicy i współpracownicy zobowiązani są do przestrzegania postanowień Polityki.

1.10. Naruszanie RODO i ustawy o ochronie danych osobowych zagrożone jest następującymi konsekwencjami karnymi:

- nieuprawnione przetwarzanie danych osobowych lub przetwarzanie danych osobowych, których przetwarzanie jest niedopuszczalne, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2,
- w przypadku, gdy nieuprawnione przetwarzanie lub przetwarzanie danych osobowych, których przetwarzanie jest niedopuszczalne, dotyczy „danych szczególnej kategorii", sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3,
- wszystkie osoby udaremniające lub utrudniające kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych, podlegają grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

2. Podstawowe definicje

2.1. **Administrator Danych (ADO)** – osoba fizyczna lub prawna, organ publiczny, jednostka 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.

2.2. **Osoba odpowiedzialna** – osoba wyznaczona przez ADO do nadzorowania przestrzegania zasad ochrony danych osobowych.

2.3. **Dane osobowe** – 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.

2.4. **Dane szczególnej kategorii** - dane ujawniające 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.

2.5. **PUODO** - Prezes Urzędu Ochrony Danych Osobowych (organ właściwy w sprawie ochrony danych osobowych/organ nadzorczy).

2.6. **Integralność**– przetwarzanie w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

2.7. **Rozliczalność –** konieczność wykazania przez administratora przestrzegania przepisów prawa z uwagi na spoczywającą na nim w tym zakresie odpowiedzialność.

2.8. **Naruszenie ochrony danych osobowych** - 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.

2.9. **Nośniki danych** – wszelkie nośniki, na których informacje zapisane są w postaci elektronicznej, w szczególności dyski, dyski CD-ROM, karty magnetyczne lub pamięci przenośne.

2.10. **Teletransmisja –** przesyłanie informacji za pomocą sieci telekomunikacyjnej.

2.11. **Proces uwierzytelniania –** działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

2.12. **Odbiorca danych** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

2.13. **Ograniczenie przetwarzania** - oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.

2.14. **Podmiot przetwarzający** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

2.15. **Poufność danych** - właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.

2.16. **Profilowanie** - dowolna forma 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.

2.17. **Przetwarzanie danych osobowych** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka 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.

2.18. **Pseudonimizacja** - 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.

2.19. **System informatyczny** – zespół urządzeń, sprzętu komputerowego, oprogramowania oraz baz danych przetwarzających dane osobowe.

2.20. **Zgoda –** zgoda osoby, której dane dotyczą oznacza 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.

2.21. **HQS SYSTEMS SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ** z siedzibą w Poznaniu, przy ul. Pasieki 24, 61-657 Poznań, wpisana do Krajowego Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy Poznań – Nowe Miasto i Wilda w Poznaniu, VIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: 0000792090 , NIP: 7831802987 , REGON: 383708759.

3. Administrowanie danymi osobowymi

Administrowanie danymi osobowymi realizowane jest poprzez:

3.1. Szacowanie ryzyka przetwarzania danych oraz ocenę skutków ich przetwarzania (potencjalnych szkód). Takim ryzykiem może być zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie, nieuprawniony dostęp do danych. Celem dokonania minimalizacji ryzyka jest dobranie odpowiednich (wynikających z tego ryzyka) środków technicznych i organizacyjnych chroniących dane.

3.2. Zapewnienie środków technicznych i organizacyjnych do ochrony przetwarzanych danych osobowych, odpowiednio do zagrożeń oraz kategorii danych objętych ochroną, w szczególności zapewnienie odpowiedniego bezpieczeństwa danych i zabezpieczenie danych przed:

- niedozwolonym lub niezgodnym z prawem przetwarzaniem,
- udostępnieniem osobom nieupoważnionym,
- zabraniem przez osobę nieuprawnioną,
- zmianą, utratą, uszkodzeniem lub zniszczeniem.

3.3. Zapewnienie legalności przetwarzania danych osobowych, a w szczególności zadbanie, by:

- spełniona została przesłanka dopuszczająca przetwarzanie danych osobowych (np. została pozyskana zgoda osoby, której dane dotyczą lub została spełniona inna przesłanka dopuszczająca przetwarzanie danych osobowych, np. przetwarzanie na podstawie zezwalających przepisów prawa),
- został spełniony obowiązek informacyjny wobec osoby, której dane dotyczą,
- dane były przetwarzane zgodnie z obowiązującymi przepisami prawa oraz normami i dobrymi praktykami oraz normami społecznymi, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (zasada zgodności z prawem, rzetelności i przejrzystości),
- dane zbierane były w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami (zasada ograniczenia celu),
- dane były merytorycznie poprawne i w razie potrzeby uaktualniane (uprawnienia korekcyjne), a gdy dane osobowe są nieprawidłowe w świetle celów ich przetwarzania – zadbanie, by zostały one niezwłocznie usunięte lub sprostowane (zasada prawidłowości), a osoba, której dane dotyczą, mogła realizować swoje prawa w stosunku do nich,
- zakres danych był adekwatny, stosowny oraz ograniczony do tego, co niezbędne do celów, w których są przetwarzane (zasada minimalizacji danych),
- były przetwarzane z ograniczeniem czasowym, przez co rozumiane jest przechowywanie w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane (zasada ograniczenia przechowywania),
- ochrona danych osobowych była traktowana jako domyślne ustawienie każdego programu czy projektu. Procedury uruchamiania nowych projektów i inwestycji uwzględniają konieczność oceny wpływu zmiany na ochronę danych, zapewnienie prywatności (w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu *(privacy by design)*.

3.4. Zapewnienie minimalizacji przetwarzanych danych pod kątem adekwatności danych do celów (ilości danych i zakresu przetwarzania), dostępu do danych, czasu przechowywania danych.

- Minimalizacja zakresu

- zweryfikowano zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO,
- Nie rzadziej niż co 3 lata dokonywany jest okresowy przegląd ilości przetwarzanych danych i zakresu ich przetwarzania,
- Przeprowadzana jest weryfikacja zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (*privacy be design*).

- Minimalizacja dostępu
  - Stosowane są ograniczenia dostępu do danych osobowych: prawne (zobowiązania do poufności, zakresy upoważnień), fizyczne (strefy dostępu, zamykanie pomieszczeń) i logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których przechowywane są dane osobowe)
  - Dokonywana jest aktualizacja uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób oraz zmianach podmiotów przetwarzających
- Minimalizacja czasu
  - Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów informatycznych, a ich wersje papierowe są niszczone w sposób mechaniczny za pomocą niszczarki dokumentów.
  - Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez ADO.

3.5. Główna działalność ADO nie polega na przetwarzaniu Danych szczególnej kategorii.

3.6. Prowadzenie dokumentacji opisującej sposób przetwarzania danych osobowych, w szczególności:

- Polityki bezpieczeństwa danych osobowych,
- Rejestru czynności przetwarzania danych osobowych. Wzór rejestru stanowi załącznik 7 do niniejszej Polityki.
- Polityki Prywatności i Cookies.

3.7. W ramach działalności ADO prowadzone są następujące zbiory danych:

1) **dane osobowe osób fizycznych – Klientów,** których dane osobowe są przetwarzane w oparciu o art. 6 ust. 1 lit. b RODO, tj. w związku z podjęciem działań na żądanie osoby, której dane dotyczą, a w dalszym etapie w związku z realizacją zawartej umowy,
2) **dane osobowe osób reprezentujących podmioty prawne będące Klientami Administratora** – dane osobowe są przetwarzane w oparciu o art. 6 ust. 1 lit. b RODO, tj. w związku z podjęciem działań na żądanie osoby, której dane dotyczą, a w dalszym etapie w związku z realizacją zawartej umowy
3) **dane osobowe osób fizycznych** – w związku z korzystaniem z usługi polegającej na bezpłatnej konsultacji z Administratorem w związku ze świadczoną usługą przetwarzane są dane osób fizycznych zapisujących się na bezpłatne konsultacje w oparciu o art. 6 ust. 1 lit. a RODO, tj. na podstawie udzielonej zgody,
4) **dane osobowe kandydatów do zatrudnienia** są przetwarzane w oparciu o art. 6 ust. 1 lit. a RODO, tj. na podstawie zgody kandydata na przetwarzanie jego danych osobowych na potrzeby przyszłych

rekrutacji oraz na podstawie art. 6 ust. 1 lit. b RODO, tj. w związku z podjęciem działań na żądanie osoby, której dane dotyczą,

5) **dane osobowe osób fizycznych Pracowników/Współpracowników** przetwarzane są w oparciu o art. 6 ust. 1 lit. b RODO, tj. w związku z zawartą umową o pracę lub umową cywilnoprawną,

6) **dane osobowe osób fizycznych – Reprezentantów Kontrahentów** są przetwarzane w oparciu o art. 6 ust. 1 lit. f RODO, tj. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora, ,

7) **dane osobowe osób fizycznych – Użytkowników** korzystających z serwisu Facebook, Google, LinkedIn a w szczególności obserwujące profil Administratora, które przetwarzane są na podstawie art. 6 ust. 1 lit. f RODO tj. na podstawie uzasadnionego interesu Administratora.

ADO prowadzi Rejestr czynności przetwarzania w celu spełnienia ciążącego na nim obowiązku wynikającego z RODO, a także w celu sprawowania bieżącej kontroli nad przetwarzaniem danych w swoim przedsiębiorstwie.

3.8. W Rejestrze czynności przetwarzania danych osobowych wyróżnia się m.in. takie pozycje jak: kategorie osób, których dane są przetwarzane, kategorie przetwarzanych danych, cel przetwarzania danych, kategorie odbiorców, którym dane są/będą ujawnione, a także planowane terminy usunięcie kategorii przetwarzanych danych. ADO udostępni Rejestr czynności przetwarzania na żądanie organu nadzorczego.

3.9. Wyznaczenie Osoby odpowiedzialnej za nadzorowanie przestrzegania zasad ochrony w przypadku, w którym ADO nie wykonuje tych obowiązków sam.

Osobą odpowiedzialną w przypadku ADO jest Wojciech Świdurski – tel. +48 661 339 731, e-mail: rodo@hqs.cloud

3.10. W ramach swojej działalności ADO nie dokonuje profilowania.

3.11. Wydawanie i zarządzanie upoważnieniami do przetwarzania danych osobowych, w tym w szczególności dopuszczanie do przetwarzania danych wyłącznie osoby przeszkolonej i posiadającej upoważnienie do przetwarzania danych osobowych, która zobowiązała się do zachowania poufności. Upoważnienia do przetwarzania danych osobowych są nadawane przez Właściciela. Wzór upoważnienia wraz z oświadczeniem o zachowaniu poufności stanowi załącznik nr 4 do niniejszej Polityki.

3.12. Nadzorowanie i dbanie o zgodne z prawem przekazywanie danych osobowych (udostępnianie i powierzanie).

3.13. Respektowanie prawa osób, których dane dotyczą, a w szczególności prawa do uzyskania informacji przy pozyskiwaniu danych osobowych o:

- administratorze danych oraz osobie odpowiedzialnej za nadzorowanie przestrzegania ochrony danych osobowych u ADO lub o Inspektorze Ochrony Danych, jeżeli został powołany,
- celu przetwarzania danych oraz podstawie prawnej przetwarzania,
- okresie przetwarzania danych,
- sposobie udostępniania danych oraz ich odbiorcach, w tym państwach trzecich, jeżeli takie udostępnienie ma nastąpić,
- uprawnieniach osoby w zakresie danych osobowych,
- prawie wniesienia skargi do PUODO,
- stosowaniu profilowania, jeżeli takie jest wykorzystywane,

- tym czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są konsekwencje niepodania danych,
- źródle pochodzenia danych osobowych i kategoriach przetwarzanych danych, jeżeli dane nie pochodzą od osoby, której dotyczą.

3.14. Respektowanie praw osób, których dane dotyczą w zakresie:

- dostępu do danych: uprawnienie osoby, której dane dotyczą, polegające na uzyskaniu potwierdzenia, czy jej dane podlegają przetwarzaniu, a jeżeli tak, to do uzyskania dostępu do nich oraz informacji w jaki sposób przetwarzanie się odbywa,
- sprostowania danych: uprawnienie osoby, której dane dotyczą polegające na możliwości żądania niezwłocznego sprostowania danych jej dotyczących,
- usunięcia danych („prawo do bycia zapomnianym"): uprawnienie polegające na możliwości żądania niezwłocznego usunięcia danych osobowych dotyczących osoby wnoszącej żądanie,
- ograniczenia przetwarzania: uprawnienie osoby, której dane dotyczą polegające na żądaniu ograniczenia przetwarzania jej danych,
- przenoszenia danych: uprawnienie osoby, której dane dotyczą polegające na żądaniu przeniesienia jej danych bezpośrednio do innego administratora, pod warunkiem, że przetwarzanie danych odbywa się na podstawie zgody albo na podstawie umowy, w sposób zautomatyzowany,
- wniesienia sprzeciwu: uprawnienie osoby, której dane dotyczą dające możliwość wniesienia w każdym momencie sprzeciwu – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych opartego na art. 6 ust. 1 lit. e) lub f) Ogólnego Rozporządzenia o Ochronie Danych Osobowych.

3.15. Przeprowadzanie regularnych wewnętrznych audytów przestrzegania przepisów dotyczących ochrony danych osobowych, przy czym ADO określa, że regulacje wewnętrzne będą podlegały przeglądaniu corocznie do końca grudnia, a także każdorazowo w razie zmiany w działalności ADO mogącej mieć istotny wpływ na ryzyko naruszeń przetwarzanych danych osobowych.

4. Osoba odpowiedzialna za nadzorowanie przestrzegania ochrony danych osobowych u ADO

4.1. Osoba odpowiedzialna lub sam ADO realizuje swoje obowiązki w oparciu o RODO, ustawę o ochronie danych osobowych, ustawy szczególne, rozporządzenia wykonawcze oraz wewnętrzne regulacje ADO, służące do przetwarzania danych osobowych.
4.2. Osoba odpowiedzialna jest niezależna w wykonywaniu zadań z zakresu ochrony danych osobowych.
4.3. ADO zapewnia, by Osoba odpowiedzialna była właściwie i niezwłocznie włączana we wszystkie sprawy dotyczące ochrony danych osobowych.
4.4. Osoba odpowiedzialna ma dostęp do całości gromadzonych i przetwarzanych danych osobowych w zakresie niezbędnym do realizacji zadań. ADO wspiera Osobę odpowiedzialną w wypełnianiu jego zadań, zapewniając zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.
4.5. Osoba odpowiedzialna jest zobowiązana do zachowania poufności co do wykonywania swoich zadań.
4.6. Osoba odpowiedzialna wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

4.7. Osoba odpowiedzialna odpowiada za realizację całokształtu spraw związanych z nadzorem nad przestrzeganiem zasad ochrony związanych z zastosowaniem środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności:

- sprawuje nadzór nad fizycznym zabezpieczeniem danych osobowych przed zabraniem przez osobę nieuprawnioną, zmianą, utratą, uszkodzeniem lub zniszczeniem,
- nadzoruje, czy do przetwarzania danych osobowych zostały dopuszczone wyłącznie osoby posiadające pisemne upoważnienie nadane przez ADO,
- informuje ADO, podmiot przetwarzający oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów o ochronie danych i doradza im w tej sprawie,
- monitoruje przestrzeganie RODO i innych przepisów o ochronie danych oraz polityk ADO w zakresie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,
- udziela na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitoruje jej wykonanie,
- współpracuje z organem nadzorczym,
- zapewnia kontrolę nad zgodnym z prawem zbieraniem danych osobowych oraz ich przekazywaniem,
- opracowuje i aktualizuje Politykę bezpieczeństwa danych osobowych,
- prowadzi ewidencję upoważnień do przetwarzania danych osobowych oraz oświadczeń o zachowaniu poufności, której wzór stanowi załącznik nr 3 do niniejszej Polityki
- na zlecenie ADO powiadamia PUODO o stwierdzonym naruszeniu danych osobowych, jak i również informuje podmiot danych, którego dotyczy naruszenie,
- na żądanie osoby, której dane dotyczą, przygotowuje wniosek dla ADO o udzielenie odpowiedzi lub realizacji innych praw,
- sprawuje nadzór nad systemem informatycznym służącym do przetwarzania danych osobowych, w szczególności w zakresie:
    - nadawania uprawnień,
    - stosowanych metod i środków uwierzytelniania,
    - sposobu rozpoczęcia, zawieszenia i zakończenia pracy w systemie,
    - procesu tworzenia kopii zapasowych,
    - sposobu i miejsca przechowywania nośników informacji zawierających dane osobowe,
    - sposobu zabezpieczenia systemu przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu,
    - utraty danych spowodowaną awarią zasilania,
    - przetwarzania danych na komputerach przenośnych,
    - spełniania przez system wymagań nakładanych przez prawo na systemy przetwarzające dane osobowe w zakresie odnotowywania informacji,

- likwidacji, przekazania lub naprawie urządzeń lub nośników zawierających dane osobowe,
- ochrony systemu przed zagrożeniami pochodzącymi z sieci publicznej.

- informuje ADO o stwierdzonych przypadkach naruszenia bezpieczeństwa danych osobowych,
- konsultuje się z ADO w sprawie oceny skutków dla ochrony danych,
- na zlecenie ADO uczestniczy w czynnościach kontrolnych PUODO,
- dokonuje ciągłej oceny stanu ochrony danych osobowych, przedstawiając wnioski ADO.

4.8. Podczas realizacji swych zadań, Osoba odpowiedzialna ma prawo do:

- uzyskiwania wszelkich informacji dotyczących przetwarzanych danych osobowych od wszystkich komórek organizacyjnych,
- kontrolowania komórek organizacyjnych pod kątem właściwego zabezpieczenia pomieszczeń oraz systemów informatycznych, w których przetwarzane są dane,
- proponowania ADO rozwiązań dotyczących ochrony danych osobowych,
- wydawania orzeczeń dotyczących właściwego zbierania i przekazywania danych osobowych,
- wydawania poleceń kierownikom komórek organizacyjnych w zakresie bezpieczeństwa danych osobowych,
- żądania od wszystkich pracowników udzielenia wyjaśnień w sytuacjach naruszenia bezpieczeństwa danych osobowych lub w związku z nieprawidłowościami lub zagrożeniami związanymi z ochroną danych osobowych.

5. Powierzenie przetwarzania danych osobowych

5.1. ADO może powierzyć przetwarzanie w swoim imieniu danych osobowych innemu podmiotowi przetwarzającemu w drodze umowy zawartej w formie pisemnej. W tym zakresie ADO korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi przepisów o ochronie danych osobowych i chroniło prawa osób, których dane dotyczą.

5.2. ADO przyjął minimalne wymagania co do umowy powierzenia przetwarzania danych stanowiące Załącznik nr 1a oraz nr 1b do niniejszej Polityki – „Wzór umowy powierzenia przetwarzania danych".

5.3. ADO prowadzi rejestr podmiotów, którym powierzył przetwarzanie w swoim imieniu danych osobowych. Wzór rejestru stanowi załącznik nr 2 do niniejszej Polityki – „Podmioty, którym powierzono przetwarzanie danych osobowych".

5.4. Podmiot przetwarzający, któremu powierzono przetwarzanie danych obowiązany jest wykorzystywać powierzone mu dane wyłącznie w celach i w zakresie, które zostały wskazane w zawartej z nim umowie.

5.5. Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej zgody ADO. ADO może jednak wyrazić zgodę ogólną w umowie powierzenia,

z zastrzeżeniem, że podmiot przetwarzający poinformuje o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym ADO możliwość wyrażenia sprzeciwu wobec takich zmian.

5.6. Przetwarzanie danych osobowych przez inny podmiot przetwarzający, w sytuacji dalszego powierzenia danych do przetwarzania przez pierwotny podmiot przetwarzający, oparte jest według umów zawartych z tym podmiotem o poniższe zasady.

Podmiot przetwarzający, któremu powierzono przetwarzanie danych obowiązany jest w szczególności do:

- stosowania odpowiednich środków ochrony danych osobowych, w tym do zapewnienia fizycznej ochrony pomieszczeń w których przetwarzane są dane oraz tworzenia kopii bezpieczeństwa systemów informatycznych, w których przetwarzane są powierzone dane osobowe;
- opracowania i wdrożenia dokumentacji dotyczącej przetwarzania danych osobowych, w szczególności polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym, o ile zaistnieją ku temu przesłanki;
- niezwłocznego powiadomienia ADO o przypadkach naruszenia przetwarzania powierzonych danych osobowych oraz do dokumentowania wszelkich informacji, które mogą pomóc w ustaleniu okoliczności tego naruszenia;
- niezwłocznego poinformowania ADO, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie przepisów o ochronie danych osobowych;
- wdrożenia procedur pozwalających niezwłocznie i zgodnie z prawem realizować ADO obowiązki dostępu do danych osobowych osób, których dotyczą oraz uprawnień korekcyjnych, w tym udzielanie odpowiedzi osobie, która chce skorzystać ze swoich praw w ciągu miesiąca od chwili, gdy ADO otrzyma takie żądanie;
- zapewnienia, aby każdy pracownik/współpracownik podmiotu przetwarzającego przetwarzający powierzone dane osobowe posiadał pisemne upoważnienie do przetwarzania tych danych osobowych i zobowiązał się do zachowania poufności;
- udostępnienia na każde żądanie ADO informacji na temat sposobów przetwarzania i zabezpieczenia powierzonych danych osobowych, wraz zapewnieniem możliwości wglądu i inspekcji do pomieszczeń lub procedur podmiotu przetwarzającego (audyty podmiotu przetwarzającego);
- po stwierdzeniu naruszenia ochrony danych osobowych – zgłoszenia ich ADO bez zbędnej zwłoki wraz z określeniem okoliczności i podjętych środków zaradczych;
- po zakończeniu świadczenia usług związanych z przetwarzaniem - na żądanie ADO – usunięcia lub zwrotu mu wszelkich danych osobowych oraz usunięcia wszelkich ich istniejących kopii, chyba że przepisy prawa nakazują przechowywanie takich danych osobowych.

5.8 Jeżeli podmiot przetwarzający powierzył dane do przetwarzania, a inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec ADO za wypełnienie obowiązków tego innego podmiotu spoczywa na pierwotnym podmiocie przetwarzającym.

6. Zarządzanie naruszeniami ochrony danych

6.1 Każdy z pracowników/współpracowników jest zobowiązany do poinformowania ADO w sytuacji podejrzenia lub stwierdzenia przez niego naruszenia ochrony danych osobowych.

6.2 ADO może uzyskać informację o wystąpieniu naruszenia także w inny sposób, w szczególności ze źródła zewnętrznego.

6.3 W momencie pozyskania przez ADO informacji o podejrzeniu lub wystąpieniu naruszenia ochrony danych osobowych Osoba odpowiedzialna rozpoczyna postępowanie wyjaśniające, którego celem jest ustalenie przyczyn wystąpienia naruszenia, jego przebiegu oraz skutków.

6.4 W ramach prowadzonego postępowania wyjaśniającego Osoba odpowiedzialna współpracuje z komórkami merytorycznymi zaangażowanymi w wyjaśnianie Incydentu. Ze względu na ścisły reżim czasowy na jego weryfikację przedstawiciele wskazanych komórek organizacyjnych zobowiązani są pozostać do dyspozycji Osoby odpowiedzianej niezależnie od obowiązków wynikających z procesów merytorycznych.

6.5 W wyniku przeprowadzonego postępowania wyjaśniającego Osoba odpowiedzialna przekazuje ADO (nie później, niż w ciągu 48 h od podejrzenia lub wystąpienia naruszenia) informacje, które udało jej się ustalić w trakcie postępowania wraz z rekomendacją:

- czy o wystąpieniu naruszenia należy zawiadomić organ nadzorczy,
- czy należy zawiadomić osoby, których dane zostały naruszone,
- jakie działania należy podjąć, aby zminimalizować skutki naruszenia,
- jakie działania należy podjąć, aby zapobiec wystąpieniu podobnego naruszenia w przyszłości.

6.6 ADO podejmuje decyzję co do przedstawionych mu rekomendacji oraz zleca ich realizację odpowiednim osobom.

6.7 W przypadku decyzji o konieczności zgłoszenia naruszenia do organu nadzorczego, **zgłoszenie następuje najpóźniej w ciągu 72 h od stwierdzenia naruszenia**. Zgłoszenie zawiera co najmniej:

- opis charakteru naruszenia ze wskazaniem kategorii i przybliżonej liczby osób, których dane dotyczą oraz kategorie i przybliżoną liczbę wpisów, których naruszenie dotyczy,
- imię i nazwisko oraz dane kontaktowe osoby, z którą należy się kontaktować w sprawie naruszenia,
- opis możliwych konsekwencji naruszenia danych osobowych,
- opis zastosowanych środków lub proponowanych w celu zaradzenia naruszeniom na przyszłość oraz opis zastosowanych środków w celu zminimalizowania skutków naruszenia w czasie rzeczywistym.

6.8 W przypadku decyzji o konieczności zawiadomienia osób, których dane zostały naruszone, zawiadomienie zawiera co najmniej informacje, o których mowa w punkcie 6.7

6.9 Osoba odpowiedzialna prowadzi rejestr stwierdzonych naruszeń. Wzór rejestru stanowi załącznik nr 5 do niniejszej Polityki.

7. Realizacja praw osób, których dane dotyczą

7.1 O wpłynięciu wniosku o realizację praw osób, których dane dotyczą należy niezwłocznie poinformować Osobę odpowiedzialną nie później niż w terminie 3 dni od daty jego wpłynięcia.

7.2 Wniosek jest realizowany w terminie 14 dni od dnia jego wpłynięcia. Termin ten może zostać przedłużony o kolejne miesiąc z uwagi na skomplikowany charakter żądania lub liczbę żądań. W

przypadku wydłużenia terminu, w terminie 14 dni od dnia wpłynięcia wniosku należy poinformować podmiot danych o wydłużeniu terminu oraz podać przyczyny opóźnienia.

7.3 Odpowiedź na wniosek udzielana jest w formie, w której zostało sformułowane żądanie, chyba że osoba wnioskująca wskaże preferowaną inną formę kontaktu.

7.4 Odpowiedzi na wniosek udziela Osoba odpowiedzialna w porozumieniu z Zarządem.

7.5 Każdorazowe wpłynięcie wniosku oraz zakres jego realizacji jest odnotowywany w rejestrze wniosków o realizację praw osób, za którego prowadzenie odpowiedzialny Osoba odpowiedzialna. Wzór rejestru został określony w załączniku nr 6 do niniejszej Polityki.

ROZDZIAŁ II Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych

1 Środki ochrony fizycznej i organizacyjnej

1.1. Zasady postępowania z danymi osobowymi

Szczególne zasady postępowania z danymi osobowymi:

- wszelkie miejsca, gdzie przechowuje się nośniki danych osobowych (szafy z dokumentami, szafy komputerowe z nośnikami, itp.) są odpowiednio zabezpieczone bez możliwości dostępu osób nieuprawnionych do przetwarzania tych danych, tj. zamknięte na klucz (tutaj:, dane pracowników/współpracowników, dane Klientów będących osobami fizycznymi, dane osób reprezentujących Klientów będących osobami prawnymi, dane Kontrahentów),

- przebywanie osób trzecich w pomieszczeniach, gdzie są przetwarzane dane osobowe, dopuszczalne jest tylko w obecności pracownika/współpracownika upoważnionego do przetwarzania tych danych lub za zgodą ADO,

- ogranicza się ilość osób uprawnionych do panelu administracyjnego strony internetowej (w razie zmiany osoby uprawnionej, np. odejścia pracownika/współpracownika, dokonuje się zmiany haseł dostępowych),

- monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane,

- ADO stosuje tzw. politykę czystego biurka i czystej drukarki, zgodnie z którą na biurkach i urządzeniach (w szczególności drukarkach i kopiarkach) nie powinny znajdować się nieużywane lub pozostawione bez nadzoru osoby upoważnionej dokumenty i nośniki zawierające dane osobowe,

- dostęp do pomieszczeń, w których przetwarzane są dane, mogą mieć dostęp osoby nieupoważnione do przetwarzania danych, takie jak np. rodzina. W celu zminimalizowania ryzyka wynikającego z tego stanu: osoba nieupoważniona może przebywać w takim pomieszczeniu tylko pod nadzorem osoby upoważnionej.

- dokumenty w formie papierowej zawierające dane osobowe skanowane są do wyznaczonego folderu na serwerze komputera dostępnego tylko dla osób uprawnionych do wglądu w te dane,

- dostęp do programu księgowego ograniczony jest okresowo zmienianym hasłem,

- nośniki zawierające dane osobowe i przeznaczone do likwidacji pozbawia się wcześniej zapisu tych danych w sposób trwały, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich późniejsze odczytanie, w przypadku dokumentacji papierowej – usuwa się w niszczarce dokumentów lub z wykorzystaniem zewnętrznej firmy utylizującej dokumentację w sposób gwarantujący skuteczne usunięcie, co potwierdzane jest stosownym certyfikatem, protokołem poświadczającym likwidację lub w inny sposób zapewniający rozliczalność,

- dokumenty z danymi osobowymi są przechowywane w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności na włamanie,

- nośniki zawierające dane osobowe i przeznaczone do przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,

- nośniki zawierające dane osobowe i przeznaczone do naprawy — są przekazywane do serwisu dokonującego naprawy, z zastrzeżeniem wcześniejszego zaszyfrowania nośnika danych bądź usunięcia nośników danych,

- współpracuje się ze sprawdzonymi podmiotami przetwarzającymi dane osobowe oraz odbiorcami danych, zobowiązując ich do poufności i najwyższych standardów,

- użytkownik urządzenia przenośnego (m.in. laptop, nośniki zewnętrzne) zawierającego dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania oraz użytkowania poza siedzibą,

- dostosowywanie się do wyników audytu,

1.2. Osoby zatrudnione (lub osoby upoważnione do przetwarzania danych w Spółce, w oparciu o inny status niż umowa o pracę)

Osoby zatrudnione przy przetwarzaniu danych osobowych:

- zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych, co potwierdzają podpisanym przez siebie oświadczeniem,

- przeszkolono w zakresie zabezpieczeń systemu informatycznego, co potwierdzają podpisanym przez siebie oświadczeniem,

- zostały obowiązane do zachowania ich w tajemnicy, co potwierdzają podpisanym przez siebie oświadczeniem,

- dane pracowników i współpracowników są przechowywane w szafie zamykanej na klucz lub ewentualnie szafie pancernej, do której mają dostęp tylko osoby zarządzające,

- mają pisemne, imienne upoważnienia ADO ze wskazaniem zakresu danych osobowych, do którego mają dostęp.

2 Środki sprzętowe oraz narzędzi programowych

2.1. Środki infrastruktury informatycznej i telekomunikacyjnej

ADO wdraża odpowiednie techniczne środki ochrony danych osobowych uwzględniające stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze.

Do zabezpieczenia danych osobowych przetwarzanych w systemach informatycznych zastosowano następujące środki infrastruktury informatycznej i telekomunikacyjnej:

- dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła:
  - zabezpieczenie wszystkich stacji roboczych hasłami „trudnymi" (min. 8 znaków w tym litery, cyfry, znaki dodatkowe) zmienianymi nie rzadziej niż co 3 miesiące,
  - wymuszenie wylogowania po 30 minutach bezczynności użytkownika stacji roboczej,
- zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji (np. szyfrowanie dokumentów z danymi przesyłanych e-mailem poprzez dostarczanie hasła inną drogą komunikacji),
- zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity na każdej stacji roboczej,
- użyto system Firewall do ochrony dostępu do sieci komputerowej, który jest regularnie i ręcznie aktualizowany przez ADO,
- serwer poczty elektronicznej zlokalizowany jest i obsługiwany przez inny podmiot,
- zastosowano szyfrowanie dysków w komputerach przenośnych,
- Serwer przechowywany jest na terenie UE, we współpracy z podmiotem dysponującym infrastrukturą odpowiednią do zabezpieczenia danych i odpowiedzi na ewentualne awarie (podstawy umowne),
- komunikacja zdalna pomiędzy stacją roboczą a serwerem, na którym przetwarzane są dane, odbywa się za pośrednictwem bezpiecznych kanałów. Kopie zapasowe danych osobowych wykonywane są co najmniej raz dziennie.
- wprowadzono środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach w dokumentach z danymi osobowymi (np. kont użytkownika),
- blokuje się korzystanie z prywatnych zasobów pracowników/współpracowników, tj. ściąganie plików, instalowanie urządzeń, używanie pendrive, korzystanie z prywatnych skrzynek e-mailowych – zasady blokady),
- urządzenia, na których przetwarzane są dane osobowe wyposażone są w sprawne baterie lub zasilacze UPS,
- konta pocztowe oraz strona internetowa posiadają szyfrowanie SSL.

Postanowienia końcowe

1. Polityka ma charakter wewnętrzny i może być udostępniana osobom trzecim, które nie są pracownikami lub współpracownikami Administratora wyłącznie za jego pisemną zgodą i po zawarciu stosownej umowy / klauzuli o zachowaniu poufności, z zastrzeżeniem przypadków prawem przewidzianych.

2. Każdy pracownik lub współpracownik Administratora powinien zapoznać się z treścią Polityki i złożyć pisemne oświadczenie o zobowiązaniu się do jej przestrzegania.

3. Niewykonywanie lub nienależyte wykonywanie przez pracowników obowiązków wynikających z Polityki i przepisów prawa będzie równoznaczne z ciężkim naruszeniem obowiązków pracowniczych. Nie wyklucza to możliwości poniesienia przez sprawcę odpowiedzialności karnej na podstawie ustawy o ochronie danych osobowych.

4. W zakresie nieuregulowanym w Polityce zastosowanie znajdują przepisy RODO oraz Ustawy.

5. Załączniki:

   a) Załącznik nr 1a - Wzór Umowy powierzenia przetwarzania danych osobowych jako HQS SYSTEMS SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ jako procesor,
   b) Załącznik nr 1b - Wzór Umowy powierzenia przetwarzania danych osobowych jako HQS SYSTEMS SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ jako administrator,
   c) Załącznik nr 2 - Wykaz podmiotów, którym powierzono przetwarzanie danych osobowych w ramach działalności HQS SYSTEMS SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ,
   d) Załącznik nr 3 – Wzór Rejestru upoważnień do przetwarzania danych osobowych HQS SYSTEMS SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ,
   e) Załącznik nr 4 – Zasady przetwarzania danych osobowych HQS SYSTEMS SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ,
   f) Załącznik nr 4a – Przykład upoważnienia do przetwarzania danych osobowych HQS SYSTEMS SPÓŁKA Z OGRANICZONĄ ODPOWIEDZILANOŚCIĄ
   g) Załącznik nr 5 – Rejestr naruszeń dotyczący podmiotu HQS SYSTEMS SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ,
   h) Załącznik nr 6 – Rejestr wniosków o realizację praw HQS SYSTEMS SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ,
   i) Załącznik nr 7a – Rejestr czynności przetwarzania danych osobowych dotyczący HQS SYSTEMS SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ,
   j) Załącznik nr 7b – Rejestr kategorii czynności przetwarzania danych osobowych HQS SYSTEMS SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ,

k) Załącznik nr 8 – Polityka prywatności dotyczący HQS SYSTEMS SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ,
l) Załącznik nr 8a – Wzór klauzuli informacyjnej dla kandydatów do zatrudnienia HQS SYSTEMS SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ,
m) Załącznik nr 8b – Wzór klauzuli informacyjnej dla Pracowników i Współpracowników HQS SYSTEMS SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ,
n) Załącznik nr 8c – Wzór klauzuli informacyjnej dla reprezentantów kontrahentów dotyczący HQS SYSTEMS SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ,
o) Załącznik nr 9 – Instrukcja usuwania danych osobowych dotyczący HQS SYSTEMS SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ,
p) Załącznik nr 10 – Monitorowanie i sprawdzanie przyjętych procedur ochrony danych osobowych dotyczący HQS SYSTEMS SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ,
q) Załącznik nr 11 – Zasady privacy by design oraz privacy by default dotyczące HQS SYSTEMS SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ,
r) Załącznik nr 12 – Zasady postępowania przy naruszeniach danych osobowych HQS SYSTEMS SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ,
s) Załącznik nr 13 – Zasady przetwarzania danych osobowych w systemach informatycznych HQS SYSTEMS SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ,
t) Załącznik nr 14 - Zasady przetwarzania danych osobowych w systemach tradycyjnych HQS SYSTEMS SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ.