POLITYKA OCHRONY DANYCH OSOBOWYCH
dla SmartQube Spółka z ograniczoną odpowiedzialnością
z siedzibą we Wrocławiu, ul. Rakietowa 29E, 54-615 Wrocław

Wrocław, dnia 02 stycznia 2024 r.

I. CEL I ZAKRES

1. Aby zapewnić ochronę podstawowych praw i wolności osób fizycznych, w szczególności prawo do ochrony danych osobowych, które są przetwarzane przez SmartQube Sp. z o.o. /dalej „Administrator"/, Administrator ustanawia niniejszą Politykę ochrony danych osobowych /dalej „Polityka"/.
2. Polityka określa normy postępowania osób zatrudnionych i osób współpracujących w zakresie ochrony danych osobowych.
3. Polityka uwzględnia przepisy powszechnie obowiązującego prawa w zakresie ochrony danych osobowych, w szczególności przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE)

2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE /dalej „RODO”/.

4. Przy opracowywaniu niniejszej Polityki Administrator kierował się określonymi poniżej zasadami ochrony danych osobowych:
   a) zasadą legalności, zapewniającą, że Administrator przetwarza dane osobowe w oparciu o prawidłową podstawę prawną, zgodnie z art. 6 RODO, w związku z art. 5 RODO;
   b) zasadą celowości, zapewniającą, że Administrator przetwarza dane osobowe w konkretnych, wyraźnych i prawnie usprawiedliwionych celach, zgodnie z art. 5 RODO;
   c) zasadą adekwatności, zapewniającą, że przetwarzane dane osobowe są adekwatne, stosowne oraz ograniczone do tego, co niezbędne, aby osiągnąć cel przetwarzania, zgodnie z art. 5 RODO;
   d) zasadą merytorycznej poprawności, zapewniającej, że dane osobowe są prawidłowe i w razie potrzeby uaktualniane, zgodnie z art. 5 RODO;
   e) zasadą ograniczenia czasowego, zapewniającą, że dane osobowe przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, są przechowywane przez okres nie dłuższy, niż jest to niezbędne do celów przetwarzania, zgodnie z art. 5 RODO
5. Przy tworzeniu systemu ochrony danych osobowych Administrator identyfikuje obszary przetwarzania danych osobowych, przeprowadza analizę ryzyka dotyczącą ochrony danych osobowych i w oparciu o powyższą analizę wdraża środki techniczne i organizacyjne zapewniające odpowiednie do zagrożeń bezpieczeństwo danych osobowych, szczególnie zapewniające ochronę , realizując w ten sposób wymóg zapewnienia integralności, poufności i rozliczalności danych osobowych.
6. Administrator deklaruje, że zapewnienie ochrony danych osobowych jest realizacją koncepcji mającej na celu uwzględnienie ochrony danych osobowych i bezpieczeństwa informacji we wszystkich procesach realizowanych przez Administratora i jest istotnym elementem prowadzenia działalności gospodarczej, rozwoju i osiągania celów.

II. DEFINICJE

Ilekroć w Polityce użyte zostaną niżej wymienione określenia, należy przypisać im definicje niżej wymienione.

Lp.	Określenie	Definicja
1.	Administrator danych osobowych/ Administrator	Oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.
2.	Dane osobowe	Oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
3.	Przetwarzanie danych osobowych	Oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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.
4.	RODO	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE
5.	Polityka	Niniejszy dokument Polityki ochrony danych osobowych

III. SYSTEM OCHRONY DANYCH OSOBOWYCH

1. WYKAZ ZBIORÓW DANYCH OSOBOWYCH/ PROCESÓW PRZETWARZANIA DANYCH OSOBOWYCH

1.1. W celu umożliwienia prawidłowej realizacji przepisów RODO, Administrator już na etapie projektowania procesów identyfikuje procesy, a w ramach procesów - zbiory danych osobowych (kategorie danych osobowych znajdujących się w organizacji).

1.2. Wykaz procesów i zbiorów danych osobowych przetwarzanych w ramach tych procesów stanowi załącznik nr 2 do niniejszej Polityki.

1.3. Administrator prowadzi odrębne wykazy dla zbiorów danych osobowych własnych i dla zbiorów danych osobowych powierzonych do przetwarzania przez innych administratorów danych osobowych.

2. OBSZARY PRZETWARZANIA DANYCH OSOBOWYCH

2.1. W celu zapewnienia prawidłowej ochrony danych osobowych Administrator identyfikuje, zabezpiecza i nadzoruje miejsca przetwarzania danych osobowych. Wykaz miejsc przetwarzania danych osobowych zawiera załącznik nr 3 do niniejszej Polityki.

3. ANALIZA RYZYKA

3.1. Aby zapewnić wdrożenie odpowiednich środków technicznych i organizacyjnych, administrator identyfikuje ryzyka/ zagrożenia w procesach przetwarzania danych osobowych. Ryzykiem/ zagrożeniem będzie każdy czynnik, który może spowodować niedostępność danych osobowych, utratę danych osobowych, nieuprawniony dostęp do danych osobowych lub nieautoryzowaną modyfikację danych osobowych.

3.2. Administrator, w oparciu o zidentyfikowane ryzyka/ zagrożenia, przeprowadza ich analizę w obszarze ochrony danych osobowych w celu pozyskania informacji czy wdrożone zabezpieczenia są adekwatne do istniejących - nawet potencjalnie ryzyk/ zagrożeń.

3.3. Administrator za ryzyko uznaje prawdopodobieństwo wystąpienia określonego niepożądanego zdarzenia/ zagrożenia w kontekście oczekiwanych następstw tego zdarzenia.

3.4. Administrator identyfikuje ryzyka i nimi zarządza, a co najmniej raz w roku dokonuje przeglądu zidentyfikowanych ryzyk pod kątem ich aktualności i kompletności.

3.5. Administrator przyjął jakościową metodę analizy ryzyka, wykorzystując częściowo metodę SWIFT (structured „what if" technique). Administrator do zarządzania ryzykiem wykorzystuje tabelę, której wzór stanowi Załącznik nr 4 do niniejszej Polityki.

3.6. W zarządzanie ryzykiem są zaangażowani wszyscy właściciele procesów zidentyfikowanych w ramach działalności prowadzonej przez Administratora.

3.7. Każdy właściciel procesu jest zobowiązany na bieżąco zgłaszać zidentyfikowane ryzyka do działu kadr.

3.8. Dział kadr jest odpowiedzialny za dokonanie, we współpracy z właścicielami procesów, co najmniej 1 raz w roku przeglądu ryzyk, ich spisanie w tabeli wg Załącznika nr 4 do niniejszej Polityki, ich bieżące aktualizowanie i nadzór nad procesem pracy z ryzykiem i monitorowanie ryzyka, szczególnie w obszarze weryfikacji skuteczności wdrożonych środków korygujących i naprawczych.

4. ZABEZPIECZENIA TECHNICZNE/ ORGANIZACYJNE/ FIZYCZNE

ZABEZPIECZENIA TECHNICZNE

4.1. Administrator identyfikuje zasoby infrastruktury teleinformatycznej, wdraża odpowiednie jej zabezpieczenia i monitoruje wdrożone rozwiązania.

4.2. Szczegółowe zabezpieczenia infrastruktury teleinformatycznej oraz zasady zarządzania systemem informatycznym zawiera Załącznik nr 5 do niniejszej Polityki.

ZABEZPIECZENIA ORGANIZACYJNE

4.3. Administrator wyznaczył osobę odpowiedzialną za system ochrony danych osobowych, zgodnie ze wskazaniem w rozdziale IV niniejszej Polityki.

4.4. Administrator opracował i wdrożył dokumentację ochrony danych osobowych, w tym niniejszą Politykę i załączniki. Administrator uwzględnia zasady ochrony danych osobowych w pozostałej dokumentacji, w tym m.in. w dokumentacji dotyczącej zatrudnienia.

4.5. Administrator zapewnia, że dane osobowe są przetwarzane wyłącznie przez osoby, które zostały zapoznane z zasadami ochrony danych osobowych i posiadają odpowiednie upoważnienie do przetwarzania danych osobowych, a także zostały zobowiązane do zachowania poufności w zakresie ochrony danych osobowych.

4.6. Administrator prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, zgodnie z pkt III.7. niniejszej Polityki.

4.7. Administrator poprzez wdrożenie procedury, kontroluje dostęp do obszarów przetwarzania danych osobowych. Procedurę dostępu do pomieszczeń zawiera Załącznik nr 6 do niniejszej Polityki.

4.8. Osoby zatrudnione są zobowiązane stosować politykę czystego biurka, przy wykonywaniu zadań wynikających z zatrudnienia są zobowiązane stosować obowiązujące u Administratora podstawowe zasady ochrony danych osobowych, których wykaz zawiera Załącznik nr 7 do niniejszej Polityki.

4.9. Administrator, w przypadku powierzania danych osobowych innym podmiotom, zawiera wymagane prawem umowy powierzenia przetwarzania danych osobowych.

ZABEZPIECZENIA FIZYCZNE

4.10. Administrator zabezpiecza budynki i pozostałe zasoby, aby zapewnić ochronę danych osobowych, w szczególności przed utratą i nieuprawnionym dostępem.

4.11. Wykaz zabezpieczeń fizycznych jest wskazany w Załączniku nr 3 do niniejszej Polityki.

4.12. Administrator prowadzi monitoring wizyjny wyznaczonych obszarów przetwarzania danych osobowych /wykaz kamer zawiera załącznik nr 3a/ w celu zapewnienia bezpieczeństwa i porządku oraz ochrony osób i mienia. Monitorowanie nie narusza praw i podstawowych wolności osób i uwzględnia prawo do prywatności.

5. REJESTR CZYNNOŚCI PRZETWARZANIA

5.1. W celu zapewnienia, że w odniesieniu do każdego ze zbiorów wskazanych w załączniku nr 2 do niniejszej Polityki, Administrator prawidłowo realizuje założenia niniejszej Polityki, Administrator prowadzi Rejestr czynności przetwarzania, którego wzór stanowi załącznik nr 8 do niniejszej Polityki.

6. PROJEKTOWANIE/ DOMYŚLNA OCHRONA/ ANALIZA WPŁYWU

6.1. Administrator, uwzględniając wytyczne art. 25 RODO, realizuje koncepcję ochrony danych osobowych na etapie projektowania procesu (usługi, produktu, itp.) /„zasada prywatności w fazie projektowania" - „privacy by design"/ oraz koncepcję domyślnej ochrony danych osobowych /„zasada prywatności w ustawieniach domyślnych" - „privacy by default"/ i wdraża odpowiednie środki techniczne i organizacyjne, aby te zasady zrealizować.

6.2. Zgodnie z art. 35 RODO, jeśli dany proces, a w ramach procesu przetwarzanie danych osobowych, ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności

osób fizycznych, należy dokonać oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych /"*data protection impact analysis*" - „DPIA"/.

6.3. Każdy z właścicieli procesów jest zobowiązany - przed wdrożeniem nowego procesu (usługi, produktu, itp.) do konsultacji z działem kadr w zakresie wpływu nowego procesu na prawo do prywatności osób, których dane mogą być przetwarzane w procesie i w zakresie weryfikacji poziomu ochrony danych osobowych, zarówno w odniesieniu do środków technicznych jak i organizacyjnych.

6.4. W ramach konsultacji, do analizy w/w działań, tj. „privacy by design", „privacy by default" oraz „DPIA", właściciel procesu we współpracy z działem kadr wypełnia formularz wg wzoru zamieszczonego w Załączniku nr 9 do niniejszej Polityki.

6.5. Właściciel procesu jest odpowiedzialny za nadzór nad wykonaniem działań wskazanych w w/w formularzu.

6.6. W/w zasady uwzględnia się przy każdym przeglądzie procesu i jego modyfikacji.

7. OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

7.1. Do przetwarzania danych osobowych mogą być dopuszczone osoby, które zostały zapoznane z zasadami ochrony danych osobowych i posiadają nadane upoważnienie do przetwarzania danych osobowych.

7.2. Upoważnienie nadawane jest przez Administratora lub osobę przez niego upoważnioną. Osoba upoważniona do nadawania w imieniu Administratora upoważnień do przetwarzania danych osobowych jest każdorazowo wskazywana w Załączniku nr 10 do niniejszej Polityki.

7.3. W momencie zatrudnienia, nie później niż przed dopuszczeniem do przetwarzania danych osobowych, osoba wskazana w Załączniku nr 10, w porozumieniu z bezpośrednim przełożonym osoby, dla której składany jest wniosek, sprawdza czy ta osoba została zapoznana z zasadami ochrony danych osobowych i po pozytywnej weryfikacji niezwłocznie udziela upoważnienia, w oparciu o wzór zamieszczony w Załączniku nr 11 do niniejszej Polityki.

7.4. Udzielone upoważnienia są przechowywane przez osobę wskazaną w Załączniku nr 10 w miejscu zapewniającym ochronę przed nieuprawnionym dostępem.

7.5. Osoba wskazana w Załączniku nr 10 jest zobowiązana prowadzić ewidencję udzielonych upoważnień, której wzór stanowi Załącznik nr 12 do niniejszej Polityki.

7.6. Do złożenia wniosku o zmianę zakresu nadanego upoważnienia lub cofnięcie upoważnienia w trakcie zatrudnienia stosuje się ten sam wniosek co przy wniosku o nadanie upoważnienia, z zastrzeżeniem, że wniosek nie jest składany przy ustaniu zatrudnienia; w takim wypadku upoważnienie wygasa w ostatnim dniu zatrudnienia.

8. PODMIOTY PRZETWARZAJĄCE DANE OSOBOWE

8.1. Administrator w ramach prowadzonej działalności gospodarczej, realizując niektóre z procesów, korzysta z usług innych podmiotów. W przypadkach, gdy współpraca z tymi podmiotami wiąże się z koniecznością powierzenia tym podmiotom danych osobowych do przetwarzania, Administrator już na etapie zawierania umów z tymi podmiotami identyfikuje czy dochodzi do przepływów danych osobowych i zawiera wymagane w tym zakresie umowy powierzenia danych osobowych z uwzględnieniem warunków nadzoru nad powierzonymi procesami.

8.2. Wykaz listy podmiotów, którym Administrator powierza przetwarzanie danych osobowych zawiera załącznik nr 13 do niniejszej Polityki.

9. NARUSZENIA OCHRONY DANYCH OSOBOWYCH

9.1. Zarządzanie incydentami w zakresie naruszeń ochrony danych osobowych jest traktowane przez Administratora jako jeden z istotniejszych elementów systemu bezpieczeństwa. Proces ten umożliwia na bieżąco usuwanie słabości systemu, uszczelnianie systemu bezpieczeństwa poprzez wdrażanie działań korygujących i naprawczych.

9.2. Incydent to każde działanie niezgodne z jakąkolwiek polityką/ procedurą bezpieczeństwa, a także działanie lub stan faktyczny, które - mimo braku niezgodności z politykami/ procedurami bezpieczeństwa - może stanowić potencjalne niebezpieczeństwo wystąpienia zagrożenia w obszarze ochrony danych osobowych i bezpieczeństwa informacji.

9.3. W szczególności incydentami w obszarze bezpieczeństwa informacji będą: ujawnienie danych osobowych osobom nieuprawnionym, nieautoryzowana zmiana, zniszczenie, uszkodzenie danych osobowych, błędy systemu informatycznego (np. w zakresie dostępu do danych osobowych), kradzież lub zniszczenie urządzeń przetwarzających/ przechowujących informacje oraz nośników danych, ataki na system informatyczny, naruszenie zapisów polityk/ procedur bezpieczeństwa, naruszenie zapisów umów z kontrahentami, pożar, zalanie, awaria systemu kontroli dostępu.

9.4. Postępowanie z incydentem obejmuje: identyfikację incydentu, zgłoszenie incydentu, opis incydentu i przygotowanie dokumentacji i/ lub materiałów dowodowych, analizę i ocenę incydentu, zabezpieczenie incydentu do czasu wdrożenia środków korygujących i naprawczych, postępowanie naprawcze, raport i dokumentacja.

9.5. Każda osoba, która zidentyfikuje incydent lub potencjalny incydent jest zobowiązana to zgłosić w formie mailowej (a w braku możliwości wysłania wiadomości e-mail - w formie telefonicznej lub bezpośrednio) do działu kadr. Każda osoba, która zidentyfikuje incydent jest zobowiązana do jego niezwłocznego zgłoszenia, nie później niż 4 godz. od powzięcia informacji o incydencie. Zgłoszenie incydentu następuje każdorazowo z uwzględnieniem informacji, w oparciu o wzór zgłoszenia incydentu zgodnie z załącznikiem nr 14 do niniejszej

Polityki. Wzór raportu stanowi załącznik nr 15 do niniejszej Polityki. Wzór rejestru incydentów stanowi załącznik nr 16.

9.6. Dział kadr odpowiada za przyjęcie zgłoszenia incydentu, zabezpieczenie incydentu, przeprowadzenie oceny czy doszło do incydentu, analizę incydentu, podjęcie działań korygujących i naprawczych, sporządzenie raportu, ocenę skuteczności podjętych działań korygujących i naprawczych, prowadzenie rejestru incydentów.

9.7. W ramach procesu zarządzania incydentami Administrator realizuje zobowiązania RODO w tym zakresie, wskazane w art. 33 i 34 RODO; za zgłoszenia naruszeń i zawiadomienie o naruszeniu odpowiada dział kadr.

10. REALIZACJA PRAW OSÓB, KTÓRYCH DANE OSOBOWE SĄ PRZETWARZANE

10.1. Administrator realizuje prawa osób, których dane przetwarza i w trybie art. 12 RODO udziela osobie, której dane dotyczą, na jej wezwanie, informacji o przetwarzanych danych osobowych oraz o działaniach podjętych w związku z żądaniami na podstawie przepisów art. 15-22 RODO, a także realizuje obowiązek informacyjny zgodnie z art. 13-14 RODO.

10.2. Administrator realizuje obowiązek informacyjny w przypadku zbierania danych osobowych od osoby, której dane dotyczą, w trybie art. 13 RODO (szczegółowe informacje w sprawie treści klauzul informacyjnych są wskazane w rejestrze czynności przetwarzania).

10.3. Administrator realizuje obowiązek informacyjny w przypadku pozyskania danych osobowych w sposób inny niż od osoby, której dane dotyczą, w trybie art. 14 RODO (szczegółowe informacje w sprawie treści klauzul informacyjnych są wskazane w rejestrze czynności przetwarzania).

10.4. Administrator umożliwia prawo dostępu do danych osobom, których dane dotyczą, w trybie art. 15 RODO.

10.5. Administrator realizuje prawo do sprostowania danych, w trybie art. 16 RODO, z uwzględnieniem art. 19 RODO.

10.6. Administrator realizuje prawo do usunięcia danych („prawo do bycia zapomnianym") w trybie art. 17 RODO, z uwzględnieniem art. 19 RODO.

10.7. Administrator realizuje prawo do ograniczenia przetwarzania, w trybie art. 18 RODO, z uwzględnieniem art. 19 RODO.

10.8. Administrator realizuje prawo do przenoszenia danych, w trybie art. 20 RODO.

10.9. Administrator realizuje prawo do sprzeciwu i prawo, aby nie podlegać zautomatyzowanemu podejmowaniu decyzji, w trybie art. 21 i 22 RODO.

10.10. Za realizację wszelkich wniosków w zakresie w/w uprawnień odpowiada

10.11. Wnioski osób, których dane dotyczą, w zakresie w/w uprawnień należy przekazać niezwłocznie, nie później niż w terminie 1 dnia roboczego do działu kadr/działu księgowości,

który samodzielnie lub we współpracy z właścicielem procesu weryfikuje zasadność wniosku pod kątem zgodności z RODO, a następnie udziela odpowiedzi w zakresie realizacji prawa lub odmawia realizacji prawa wraz z uzasadnieniem, w trybie i w terminie prawem przewidzianym.

11. UDOSTĘPNIANIE DANYCH OSOBOWYCH

11.1. Administrator udostępnia dane osobowe podmiotom uprawnionym na mocy przepisów prawa lub innym podmiotom, w wypadku działania w oparciu o inną niż w/w podstawę prawną, w szczególności w oparciu o zgodę osoby, której dane dotyczą.

11.2. Wszystkie udostępnienia danych, inne niż podmiotom uprawnionym na mocy przepisów prawa, są odnotowane w rejestrze udostępnień, za który odpowiada dział kadr. Wzór rejestru stanowi załącznik nr 17 do niniejszej Polityki.

12. POUFNOŚĆ DANYCH/ TAJEMNICA PRZEDSIĘBIORSTWA

12.1. Ilekroć jest mowa o danych poufnych objętych tajemnicą przedsiębiorstwa należy przez to rozumieć informacje szczególnie istotne dla Administratora, których ujawnienie bądź utrata mogłyby spowodować negatywny skutek. W szczególności do danych poufnych objętych tajemnicą przedsiębiorstwa należą: dane osobowe, w rozumieniu definicji wskazanej w RODO, informacje finansowe, handlowe, techniczne i technologiczne, wszelkie informacje o wdrożonych środkach technicznych i organizacyjnych w obszarze bezpieczeństwa informacji, informacje o kontrahentach, wdrożone polityki i procedury.

12.2. Każda osoba zatrudniona u Administratora jest zobowiązana do udziału w szkoleniu z zakresu bezpieczeństwa informacji i podpisaniu oświadczenia o zachowaniu poufności. Podczas szkolenia osoby zatrudnione są zapoznawane z podstawowymi zasadami bezpieczeństwa i są informowane o obiegu dokumentacji i formie zapoznania się z politykami/ procedurami bezpieczeństwa. Wzór oświadczenia o zachowaniu poufności stanowi załącznik nr 18 do niniejszej Polityki.

12.3. Każda osoba zatrudniona, której zadania wynikające z zatrudnienia wiążą się z przetwarzaniem danych osobowych, może przystąpić do tych zadań po odbyciu szkolenia, podpisaniu oświadczenia o zachowaniu poufności oraz po nadaniu jej upoważnienia do przetwarzania danych osobowych.

12.4. Do podstawowych obowiązków osób zatrudnionych, w obszarze bezpieczeństwa informacji, należą:

a) stosowanie przepisów prawa, szczególnie przepisów RODO i wewnętrznych polityk dotyczących przetwarzania danych osobowych
b) ochrona danych poufnych przed dostępem osób trzecich, osób nieuprawnionych, także w zakresie dostępu fizycznego

c) ochrona danych poufnych przed utratą, zniszczeniem, nieautoryzowaną zmianą, ujawnieniem osobom nieuprawnionym
d) przestrzeganie niniejszej Polityki, a także pozostałych procedur
e) przestrzeganie szczegółowych zasad bezpieczeństwa w zakresie dostępu do systemu informatycznego
f) nieujawnianie osobom nieuprawnionym wdrożonych zasad bezpieczeństwa, polityki haseł i innych rozwiązań organizacyjnych
g) niezwłoczne zgłaszanie dział kadr wszelkich incydentów w obszarze bezpieczeństwa informacji
h) niewykorzystywanie narzędzi służbowych do celów prywatnych
i) niewykorzystywanie do celów służbowych nieautoryzowanych środków przetwarzania informacji

12.5. Pracownicy posiadający dostęp do danych poufnych ponoszą odpowiedzialność porządkową i odszkodowawczą wynikającą z naruszenia zasad poufności, w oparciu o powszechnie obowiązujące przepisy prawa, w szczególności kodeksu pracy. Zawinione naruszenie obowiązku ochrony danych poufnych może stanowić podstawę do dyscyplinarnego rozwiązania z pracownikiem umowy o pracę.

12.6. Osoby współpracujące na innej podstawie niż umowa o pracę odpowiadają za naruszenie zasad niniejszej procedury na zasadach ogólnych.

IV. POSTANOWIENIA KOŃCOWE

1. Niniejsza Polityka zastępuje wszystkie wcześniejsze wersje i wydania dokumentu w tej samej sprawie.
2. Nadzór nad bieżącym stosowaniem Polityki pełnią wszyscy szefowie komórek organizacyjnych.
3. Nadzór kompleksowy nad realizacją zadań wynikających z niniejszej Polityki i dokumentów związanych pełni dział kadr.
4. Niniejsza Polityka jest dokumentem poufnym, a o jej dystrybucji każdorazowo decyduje Administrator lub dział kadr.
5. Dział kadr jest odpowiedzialny za zapewnienie, że wszystkie osoby zatrudnione przez Administratora zostaną zapoznane z systemem ochrony danych osobowych.
6. Dział kadr jest odpowiedzialny za zapewnienie aktualności niniejszej Polityki i przeprowadzanie jej cyklicznych przeglądów, nie rzadziej niż 1 raz w roku.
7. Zmiana niniejszej Polityki wymaga zgody zarządu firmy, z wyjątkiem zmiany załączników. Zmiana tych załączników wymaga jedynie adnotacji w Załączniku nr 1 Lista zmian.

V. ZAŁĄCZNIKI

1. ZAŁĄCZNIK NR 1 - LISTA ZMIAN
2. ZAŁĄCZNIK NR 2 - WYKAZ ZBIORÓW DANYCH OSOBOWYCH
3. ZAŁĄCZNIK NR 3 - WYKAZ MIEJSC PRZETWARZANIA DANYCH OSOBOWYCH
4. ZAŁĄCZNIK NR 3a - WYKAZ KAMER
5. ZAŁĄCZNIK NR 4 - ANALIZA RYZYKA
6. ZAŁĄCZNIK NR 5 - INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM
7. ZAŁĄCZNIK NR 6 - PROCEDURA DOSTĘPU DO POMIESZCZEŃ
8. ZAŁĄCZNIK NR 7 - PODSTAWOWE ZASADY OCHRONY DANYCH OSOBOWYCH
9. ZAŁĄCZNIK NR 8 - REJESTR CZYNNOŚCI PRZETWARZANIA
10. ZAŁĄCZNIK NR 9 - PROJEKTOWANIE/ DOMYŚLNA OCHRONA/ ANALIZA WPŁYWU
11. ZAŁĄCZNIK NR 10 - OSOBA UPOWAŻNIONA DO NADAWANIA UPOWAŻNIEŃ DO PRZTWARZANIA DANYCH OSOBOWYCH
12. ZAŁĄCZNIK NR 11 - UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH
13. ZAŁĄCZNIK NR 12 - EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH
14. ZAŁĄCZNIK NR 13 - WYKAZ PODMIOTÓW, KTÓRYM ADMINISTRATOR POWIERZYŁ PRZETWARZANIE DANYCH OSOBOWYCH W TRYBIE ART. 28 RODO
15. ZAŁĄCZNIK NR 14 - ZGŁOSZENIE INCYDENTU
16. ZAŁĄCZNIK NR 15 - RAPORT POSTĘPOWANIA Z INCYDENTEM
17. ZAŁĄCZNIK NR 16 - REJESTR INCYDENTÓW
18. ZAŁĄCZNIK NR 17 - REJESTR UDOSTĘPNIEŃ DANYCH OSOBOWYCH
19. ZAŁĄCZNIK NR 18 - OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI

ZAŁĄCZNIK NR 1

LISTA ZMIAN

Lp.	Data przeglądu	Wskazanie zmian w dokumencie	Informacja o publikacji zmian i dacie wejścia w życie zmiany	Uwagi	Podpis

ZAŁĄCZNIK NR 2

WYKAZ ZBIORÓW DANYCH OSOBOWYCH

(SmartQube Sp. z o. o. - administrator danych osobowych)

Lp.	Proces	Nazwa zbioru	Właściciel procesu/ zbioru	Podstawa prawna przetwarzania	Adnotacje o umieszczeniu zbioru w Rejestrze czynności przetwarzania
1	Rekrutacja pracowników	CV, listy motywacyjne	Dział kadr	art.6 ust. 1 lit. a. f. RODO	Pkt.1
2	Zatrudnienie pracownika	Pracownicy	Dział kadr	art.6 ust. 1 lit. a., b., c.,f. RODO	Pkt. 2
3	Zakup usług lub towarów od osoby fizycznej	Dostawcy	Dział księgowości	art.6 ust. 1 lit. b., f. RODO	Pkt. 3
4	Sprzedaż usług lub towarów osobie fizycznej	Klienci	Dział księgowości	art.6 ust.1 lit. b., f. RODO	Pkt. 4
5.	Zapewnienie bezpieczeństwa fizycznego	Monitoring		Art. 6 ust. 1 lit. f. RODO	Pkt 5

ZAŁĄCZNIK NR 3

WYKAZ MIEJSC PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Lokalizacja – adres	Precyzyjne określenie obszaru	Rodzaje zabezpieczeń
1.	ul. Rakietowa 29E, 54-615Wrocław	Dział kard, dział księgowości, serwerownia	Zamknięcie fizyczne, klucz lub karta dostępu, monitoring wizyjny wejścia. Fizyczna ochrona mienia. Klucze do szaf. Niszczarki dokumentów.
2.	———	———	Firma zewnętrzna – biuro rachunkowe
3.			

WYKAZ ZABEZPIECZEŃ FIZYCZNYCH

L.p.	Rodzaj zabezpieczenia	Uwagi
1.	Fizyczna ochrona osób i mienia całodobowa	
2.	Fizyczna ochrona osób i mienia poza godzinami pracy	
3.	Monitoring wizyjny	
4.	System sygnalizacji włamania i napadu	
5.	Grupa interwencyjna	
6.	System kontroli dostępu z użyciem kart dostępu	
7.	Klucze do drzwi	
8.	Klucze do szaf	
9.	Sejfy	
10.	Szafy metalowe	
11.	Szafy drewniane	
12.	Czytniki biometryczne	
13.	Czujniki ruchu	
14.	Czujniki dymu	
15.	Czujniki zalania	
16.	Rolety antywłamaniowe	
17.	Portiernia/ Recepcja	
19.	System pożarowy	
20.	Niszczarki do dokumentów	

21.	Procedura ciągłości działania na wypadek naruszeń zabezpieczeń fizycznych	

ZAŁĄCZNIK NR 3a

WYKAZ KAMER

1. Siedziba przy ul Rakietowej 29E – x kamer
2.

ZAŁĄCZNIK NR 4

ANALIZA RYZYKA

Nr ryzyka	Nazwa ryzyka	Proces/ procesy, których dotyczy ryzyko	Skutek po wystąpieniu ryzyka	Metody postępowania z ryzykiem					Dodatkowe informacje
				Akceptacja	Redukcja	Unikanie	Transfer	Konsultacja z organem nadzorczym	
1	Włamanie fizyczne	Proces 1 do 4	Brak dokumentacji w formie papierowej	Monitoring, ochrona fizyczna, klucze do szaf, kontrola dostępu do biur				nd	
2	Włamanie hakerskie	Proces 1-5	Zniszczenie dokumentacji elektornicznej, konieczość odtworzenia kopii	Kopia danych do chmury, zabezpieczenie sieci urządzeniem klasy UTM, łącze VPN, system haseł				nd	
3	Udostępnienie danych przez pracownika	Proces 1 do 5	Wypłynięcie danych	Szkolenia pracowników w zakresie tajemnicy przedsiębiorstwa, danych firmy.				nd	

ZAŁĄCZNIK NR 5
INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

1. ZASADY BEZPIECZNEGO UŻYTKOWANIA SPRZĘTU IT

1. Sprzęt IT służący do przetwarzania zbioru danych osobowych składa się z komputerów stacjonarnych, laptopów, serwerów, drukarek, telefonów komórkowych, tabletów itp.
2. Użytkownik zobowiązany jest korzystać ze Sprzętu IT w sposób zgodny z jego przeznaczeniem i chronić go przed jakimkolwiek zniszczeniem lub uszkodzeniem
3. Użytkownik zobowiązany jest do zabezpieczenia Sprzętu IT przed dostępem osób nieupoważnionych a w szczególności zawartości ekranów monitorów
4. Użytkownik ma obowiązek natychmiast zgłosić zagubienie, utratę lub zniszczenie powierzonego mu Sprzętu IT
5. Samowolne otwieranie (demontaż) Sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) do lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.

2. ZASADY KORZYSTANIA Z OPROGRAMOWANIA

1. Użytkownik zobowiązuje się do korzystania wyłącznie z oprogramowania objętego prawami autorskimi
2. Użytkownik nie ma prawa kopiować oprogramowania zainstalowanego na Sprzęcie IT przez Pracodawcę / Zleceniodawcę na swoje własne potrzeby ani na potrzeby osób trzecich
3. Instalowanie jakiegokolwiek oprogramowania na Sprzęcie IT może być dokonane wyłącznie przez osobę upoważnioną
4. Użytkownicy nie mają prawa do instalowania ani używania oprogramowania innego, niż przekazane lub udostępnione im przez Pracodawcę / Zleceniodawcę. Zakaz dotyczy między innymi instalacji oprogramowania z zakupionych dyskietek, płyt CD, programów ściąganych ze stron internetowych, a także odpowiadania na samoczynnie pojawiające się reklamy internetowe
5. Użytkownicy nie mają prawa do zmiany parametrów systemu, które mogą być zmienione tylko przez osobę upoważnioną
6. W przypadku naruszenia któregokolwiek z powyższych postanowień Pracodawca / Zleceniodawca ma prawo niezwłocznie i bez uprzedzenia usunąć nielegalne lub niewłaściwie zainstalowane oprogramowanie

3. ZASADY KORZYSTANIA Z INTERNETU

1. Użytkownicy mają prawo korzystać z Internetu w celu wykonywania obowiązków służbowych
2. Przy korzystaniu z Internetu, użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego

3. Użytkownicy mają prawo korzystać z Internetu dla celów prywatnych wyłącznie okazjonalnie i powinno być ono ograniczone do niezbędnego minimum
4. Korzystanie z Internetu dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych, a także na wydajność systemu informatycznego Pracodawcy / Zleceniodawcy
5. Użytkownicy nie mają prawa korzystać z Internetu w celu przeglądania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec obowiązujących zasad postępowania, a także grać w gry komputerowe w Internecie lub w systemie informatycznym Pracodawcy / Zleceniodawcy, ściągać z Internetu jakichkolwiek plików muzycznych lub wideo
6. W zakresie dozwolonym przepisami prawa, Pracodawca / Zleceniodawca zastrzega sobie prawo kontrolowania sposobu korzystania przez Użytkownika z internetu pod kątem wyżej opisanych zasad. Ponadto, w uzasadnionym zakresie, Pracodawca / Zleceniodawca zastrzega sobie prawo kontroli czasu spędzanego przez Użytkownika w internecie. Pracodawca może również blokować dostęp do niektórych treści dostępnych przez internet.

4. ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. System Poczty Elektronicznej jest przeznaczony wyłącznie do wykonywania obowiązków służbowych
2. Przy korzystaniu z Systemu Poczty Elektronicznej, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego
3. Użytkownicy mają prawo korzystać z Systemu Poczty Elektronicznej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
4. Korzystanie z Systemu Poczty Elektronicznej dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych, a także na wydajność Systemu Poczty Elektronicznej.
5. Użytkownik jest świadomy, że wszelkie wiadomości o charakterze prywatnym utworzone lub odebrane za pośrednictwem Systemu Poczty Elektronicznej przetwarzane są wyłącznie na jego własną odpowiedzialność. Użytkownik wyraża zgodę na prowadzenie kontroli tych wiadomości przez Pracodawcę / Zleceniodawcę. Pracodawca w tej nie będzie w tej sytuacji odpowiadać za przypadkowe naruszenie dóbr osobistych Użytkownika w postaci naruszenia tajemnicy korespondencji.
6. Użytkownicy nie mają prawa korzystać z Systemu Poczty Elektronicznej w celu przeglądania lub rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania
7. Użytkownik nie ma prawa wysyłać wiadomości zawierających informacje poufne dotyczące Pracodawcy / Zleceniodawcy, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej
8. Zakazuje się uczestnictwa w tzw. „łańcuszkach szczęścia”
9. Użytkownicy nie powinni otwierać przesyłek od nieznanych sobie osób, których tytuł nie sugeruje związku z wypełnianymi przez nich obowiązkami służbowymi.
10. Użytkownicy nie powinni uruchamiać wykonywalnych załączników dołączonych do wiadomości

przesyłanych pocztą elektroniczną.
11. W przypadku przesyłania plików danych osobowych do podmiotów zewnętrznych, Użytkownik zobowiązany jest do ich spakowania i zahasłowania (8 znaków: duże i małe litery i cyfry lub znaki specjalne). Hasło należy przesłać odrębnym mailem.

5. PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

1. Użytkownik rozpoczyna pracę z systemem informatycznym przetwarzającym dane osobowe z użyciem identyfikatora i hasła
2. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów) wgląd do danych wyświetlanych na monitorach komputerowych – tzw. Polityka czystego ekranu
3. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu.
4. Po zakończeniu pracy, użytkownik zobowiązany jest:
a. wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy
b. zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe

6. ZABEZPIECZENIA INFRASTRUKTURY INFORMATYCZNEJ I TELEKOMUNIKACYJNEJ

Zastosowano następujące zabezpieczenia:
- UPS podtrzymujący zasilanie serwera (zabezpieczenie obligatoryjne)
- Listwy przepięciowe
- Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej na serwerze
- Programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych są użytkowane z zachowaniem praw autorskich i posiadają licencje (zabezpieczenie obligatoryjne)
- Lokalizacja urządzeń komputerowych (komputerów typu PC, terminali, drukarek) uniemożliwia osobom niepowołanym (np. klientom, pracownikom innych działów,) dostęp do nich (zabezpieczenie obligatoryjne)
- Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem (identyfikatora użytkownika oraz hasła lub karty procesorowej lub kodu PIN lub tokena lub technologii biometrycznej) (zabezpieczenie obligatoryjne)
- Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych
- Zastosowano systemowe mechanizmy wymuszające okresową zmianę haseł
- Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych
- Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą

teletransmisji. (zabezpieczenie obligatoryjne)
- Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia. (zabezpieczenie obligatoryjne)
- Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity. (zabezpieczenie obligatoryjne)
- Użyto system Firewall do ochrony dostępu do sieci komputerowej (zabezpieczenie obligatoryjne)
- Użyto system IDS/IPS do ochrony dostępu do sieci komputerowej
- Automat do tworzenia regularnej kopii bezpieczeństwa, dotyczy serwerów

Ponadto, dla komputerów przenośnych zastosowano:
- Szyfrowanie transmisji, przy pracy spoza sieci LAN (zabezpieczenie obligatoryjne)
- Automat do tworzenia regularnej kopii bezpieczeństwa po zalogowaniu się do sieci

7. ZABEZPIECZENIA BAZ DANYCH I OPROGRAMOWANIA

Zastosowano następujące zabezpieczenia:

- Dostęp do zbioru baz danych wymaga uwierzytelnienia z wykorzystaniem (identyfikatora użytkownika oraz hasła lub karty procesorowej lub kodu PIN lub tokena lub technologii biometrycznej) (zabezpieczenie obligatoryjne)
- Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru - Zastosowano mechanizm blokady dostępu po kilku próbach nieudanego logowania się
- Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych
- Zastosowano mechanizm umożliwiający automatyczną rejestrację identyfikatora użytkownika i datę pierwszego wprowadzenia danych (zabezpieczenie obligatoryjne)
- Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych (zabezpieczenie obligatoryjne).
- Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych dla poszczególnych użytkowników systemu informatycznego (zabezpieczenie obligatoryjne)
- Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane (zabezpieczenie obligatoryjne)
- Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych w przypadku dłuższej nieaktywności pracy użytkownika (automatyczny wygaszacz ekranu po określonym czasie) (zabezpieczenie obligatoryjne)
- Zastosowano system antywirusowy na stanowiskach, na których przetwarzane są dane (zabezpieczenie obligatoryjne)

8. METODY I ŚRODKI UWIERZYTELNIENIA

Celem procedury jest zapewnienie, że do systemów informatycznych przetwarzających dane mają dostęp jedynie osoby do tego upoważnione.

8.1. Ogólne zasady postępowania z hasłami

1. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
2. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności
3. Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom
4. Użytkownik systemu zobowiązany jest do niezwłocznej zmiany tego hasła, gdy zostało ono ujawnione

8.2. Hasła administratora

1. Hasło administratora składa się co najmniej z 8 znaków .
2. Hasło składa się z dużych i małych liter (w haśle musi być co najmniej jedna duża i co najmniej jedna mała litera) oraz z co najmniej jednej cyfry i co najmniej jednego znaku specjalnego
3. Administrator systemu zobowiązany jest zmieniać swoje hasło nie rzadziej niż co 60 dni.
4. Administrator zobowiązany jest do przechowywania haseł administratora w sejfie pod odpowiednim nadzorem.
5. W przypadku utraty uprawnień przez osobę administrującą systemem, należy niezwłocznie zmienić hasła, do których miała dostęp

8.3. Hasła do sieci i serwera – określamy, gdy na serwerze znajdują się dane osobowe

1. Hasło dostępu składa się co najmniej z 6 znaków .
2. Hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych.
3. Zmiana hasła odbywa się co najmniej raz na 30 dni i jest wymuszana przez system.

8.4. Hasła do systemów przetwarzających dane osobowe

1. Hasło dostępu składa się co najmniej z 6 znaków.
2. Hasło składa się z dużych i małych liter oraz z cyfr lub znaków.
3. Zmiana hasła odbywa się co najmniej raz na 30 dni i jest wymuszana przez system.

9. PROCEDURA TWORZENIA KOPII ZAPASOWYCH

Przykłady procedur tworzenia kopii bezpieczeństwa przedstawiono poniżej

9.1. Tworzenie kopii bezpieczeństwa programu Kadrowo – płacowego

1. Kopie zapasowe danych kadrowo-płacowych tworzone są przez system automatycznie na kolejnym

serwerze, oraz w chmurze.
2. Kopie całościowe sporządzane są raz dziennie na kolejnym serwerze oraz chmurze.
3. Każdy kopia jest opisana datą jej sporządzenia.
5. Kopie całościowe przechowywane są przez 30 dni.
6. Dostęp do kopii mają: Główny informatyk, Firma Informatyczna nadzorująca
7. Niszczenie kopii bezpieczeństwa odbywa się poprzez trwałe skasowanie.

9.2. Tworzenie kopii bezpieczeństwa dokumentacji serwera.

1. Kopie zapasowe dokumentacji serwera tworzone są w sposób zautomatyzowany w oparciu o wykorzystanie programowej funkcji serwera.
2. Kopie bezpieczeństwa sporządzane są także dla dokumentacji gromadzonej na dyskach serwera przechowywania dokumentacji.
3. Kopie całościowe sporządzane są raz dziennie
4. Dostęp do kopii mają: Główny informatyk, Firma Informatyczna nadzorująca
5. Niszczenie kopi odbywa się przez skasowanie danych na dysku twardym.

10. PROCEDURA ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO, W TYM PRZED WIRUSAMI KOMPUTEROWYMI

10.1. Ochrona antywirusowa

Celem procedury jest zabezpieczenie systemów informatycznych przed szkodliwym oprogramowaniem (np. typu robaki, wirusy, konie trojańskie, rootkity) oraz nieautoryzowanym dostępem do systemów przetwarzających dane osobowe

1. Za zaplanowanie i zapewnienie ochrony antywirusowej odpowiada dział IT, w tym za zapewnienie odpowiedniej ilości licencji dla użytkowników
2. System antywirusowy zainstalowano na serwerze oraz na stacjach roboczych.
3. System antywirusowy zapewnia ochronę: systemu operacyjnego, przechowywanych plików, poczty wychodzącej i przychodzącej.
4. Użytkownicy zobowiązani są do skanowania plików programem antywirusowym
5. Zapewnia się stałą aktywność programu antywirusowego. Tzn. program antywirusowy musi być aktywny podczas pracy systemu informatycznego przetwarzającego dane.
6. Aktualizacja definicji wirusów odbywa się automatycznie przez system

10.2. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej

Stosowane zabezpieczenia mają na celu zabezpieczenie systemów informatycznych przed nieautoryzowanym dostępem do sieci lokalnej np. przez programy szpiegujące, hackerów

1. Za zaplanowanie, konfigurowanie, aktywowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku sieci lokalnej i sieci rozległej odpowiada dział IT
2. Stosowany jest Firewall sprzętowy, programowy na serwerze
3. Zastosowano mechanizmy kontroli dostępu do sieci w postaci: IDS/IPS do wykrywania i blokowania

ataków do sieci komputerowej
4. Sieć bezprzewodową zabezpieczono protokołem WPA wraz z filtrowaniem MAC oraz IP.
5. Zastosowano mechanizmy monitorujące przeglądanie Internetu przez użytkowników. Uwzględniają one:
• Blokowanie stron internetowych określonego typu
• Blokowanie określonych stron internetowych
• Analizę przesyłanych informacji pod kątem niebezpiecznego oprogramowania

16. PROCEDURA WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI

Celem procedury jest zapewnienie ciągłości działania systemów informatycznych przetwarzających dane osobowe oraz zabezpieczenie danych osobowych przed ich nieuprawnionym udostępnieniem.
16.1. Przeglądy i konserwacje systemu informatycznego i aplikacji
1. Dział IT odpowiada za bezawaryjną pracę systemu IT, w tym: stacji roboczych, aplikacji serwerowych, baz danych, poczty email
2. Przegląd i konserwacja systemu informatycznego powinny być wykonywane w terminach określonych przez producentów systemu lub zgodnie z harmonogramem, jednak nie rzadziej, niż raz w roku
3. Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada dział IT.
4. Dział IT odpowiada za optymalizację zasobów serwerowych, wielkości pamięci i dysków
5. Dział IT odpowiada za sprawdzanie poprawności działania systemu IT, w tym: stacji roboczych, serwerów, drukarek, baz danych, poczty email

ZAŁĄCZNIK NR 6

PROCEDURA DOSTĘPU DO POMIESZCZEŃ

1. Administrator nadzoruje proces przekazania kluczy i/ lub kart dostępu do pomieszczeń.
2. Administrator lub osoba przez niego upoważniona, w przypadku konieczności nadania danemu użytkownikowi dostępu do danego pomieszczenia - wydaje użytkownikowi klucz i/ lub kartę dostępu, odnotowując fakt przekazania w rejestrze kluczy/ kart dostępu.
3. Użytkownicy są zobowiązani do nadzoru nad otrzymanymi kluczami/ kartami dostępu, są odpowiedzialni, aby klucze/ karty dostępu nie były przekazywane innym osobom inaczej, niż za pośrednictwem Administratora. Użytkownik jest zobowiązany niezwłocznie zgłosić zgubienie lub zniszczenie klucza/ karty dostępu.
4. Wszystkie osoby przebywające w obszarach przetwarzania danych są zobowiązane reagować i zgłaszać Administratorowi wszelkie incydenty w zakresie dostępu do pomieszczeń.
5. Wszystkie osoby przebywające w obszarach przetwarzania danych są zobowiązane zapewnić w zakresie własnych możliwości, że osoby trzecie nie będą przebywały w obszarach przetwarzania danych osobowych inaczej, niż w obecności upoważnionego pracownika.

ZAŁĄCZNIK NR 7

PODSTAWOWE ZASADY OCHRONY DANYCH OSOBOWYCH

1. Każda osoba przetwarzająca dane osobowe jest zobowiązana posiadać odpowiednie upoważnienie do przetwarzania danych osobowych.
2. Każda osoba przetwarzająca dane osobowe jest zobowiązana przestrzegać zasad poufności danych osobowych i chronić dane osobowe przed przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.
3. Każda osoba zatrudniona jest zobowiązana przestrzgać zasad dostępu do pomieszczeń, w szczególności jest zobowiązana, aby nie umożliwić osobie nieuprawnionej wejścia do obszarów przetwarzania danych osobowych.
4. Każda osoba zatrudniona jest zobowiązana do niezwłocznego - w terminie 4 godzin - zgłaszania incydentów, zgodnie z obowiązującą w SmartQube Sp. z o. o. procedurą.
5. Każda osoba zatrudniona jest zobowiązana do zgłaszania zauważonych luk w systemie ochrony danych osobowych i potencjalnych incydentów.
6. Wszystkie narzędzia pracy (m.in. poczta elektroniczna, internet, komputer, drukarki, wymienne nośniki informacji) powinny być wykorzystywane wyłącznie do celów wynikających z zatrudnienia w SmartQube Sp. z o. o.
7. SmartQube Sp. z o. o. zastrzega sobie prawo do przeglądu służbowej poczty elektronicznej i korespondencji, a także monitorowania wykorzystania narzędzi pracy, m.in. w zakresie rodzaju i legalności oprogramowania, odwiedzanych stron internetowych, weryfikacji połączeń telefonów komórkowych.
8. Zabronione jest powielanie, przekazywanie jakichkolwiek informacji poufnych inaczej niż w bezpośrednim związku z wykonywaniem zadań wynikających z zatrudnienia,w szcególności zabronione jest wysyłanie na adresy prywatne lub adresy osób nieuprawnionych informacji objetych klauzulą poufności.
9. Zabronione jest samodzielne instalowanie sprzętu lub oprogramownia na komputerach SmartQube Sp. z o. o. Należy przestrzegać zasady «czystego biurka», co oznacza, że po zakończeniu pracy na biurku nie powinna znajdować się dokumentacja zawierająca dane poufne. Także w trakcie pracy, w momencie odejścia od biurka, należy zabezpieczyć dokumenty poufne przed dostępem osób nieuprawnionych. Po zakończeniu pracy dokumenatcja powinna być przechowywana w szafach zamynanych na klucz.
10. Należy przestrzegać zasady «czystego ekranu», co oznacza, że każde odejście od komputera powoduje obowiązek zablokowania widoku ekranu komputera.
11. Osoby zatrudnione korzystające ze sprzętu poza obszarem przetwarzania danych osobowych są zobowiązane dochować szczególnej staranności i zapewnić ochronę sprzętu przed kradzieżą, uszkodzeniem, zniszczeniem.
12. Zabronione jest wyrzucanie dokumentacji zawierającej dane poufne, w tym dane osobowe do koszy na śmieci. Dokumentacja taka powinna być niszczona w specjlanych niszczarkach lub przekazana do podmiotu profesjonalnie zajmującego sie niszczeniem dokumentacji.

13. Zabronione jest ujawnianie w jakimkolwiek zakresie tajemnicy haseł dostępu do systemu informatycznego.

ZAŁĄCZNIK NR 8

REJESTR CZYNNOŚCI PRZETWARZANIA [...]

Administrator danych osobowych	Invest Group DI Sp. z o.o.
Dane kontaktowe	71 360 36 41 investdi@wp.pl
Inspektor ochrony danych osobowych	nie powołano
Dane kontaktowe	nie powołano
Podstawa prawna prowadzenia rejestru	art.. 30 RODO
Data utworzenia rejestru	23.07.2018
Data aktualizacji rejestru	
Osoba odpowiedzialna za prowadzenie	
Wykaz osób uprawnionych do dostępu	zgodnie z załącznikiem nr 12

Lp.	nazwa zbioru danych osobowych	właściciel zbioru danych osobowych	podstawa prawna przetwarzania	cele przetwarzania	opis kategorii osób, których dane są przetwarzane	kategorie danych osobowych	odbiorcy danych	informacja o przekazaniu danych do państwa trzeciego	informacja o usunięciu danych osobowych	informacja o technicznych i organizacyjnych środkach bezpieczeństwa, z uwzględnieniem analizy ryzyka naruszenia przepisów o ochronie danych osobowych, szczególnie utraty i nieuprawnionego dostępu do danych osobowych	miejsca przetwarzania danych osobowych	systemy/ aplikacje, z użyciem których odbywa się przetwarzanie danych osobowych	informacja o podmiotach przetwarzających	informacja o spełnieniu obowiązku informacyjnego	informacja o osobach/ kategoriach osób, którym administrator udzielił upoważnienia do przetwarzania danych osobowych	informacja o realizacji praw osób, których dane dotyczą
	wg art. 4.6. RODO		*art. 5.1a., art.6 RODO*	*art. 5. 1b. RODO*		*art. 5.1c. RODO*	*wg art. 4.9. RODO*	*rozdz. V RODO*	*art. 5.1e. RODO*	*art. 5.1f., art. 32 RODO*			*art. 28 RODO*	*art. 13, 14 RODO*		*art. 15-22 RODO*
1.	cv, listy motywacyjne	dział kadr	art. 6 ust. 1 lit. a., f.	wybór kandydatów do zatrudnienia	osoby fizyczne - kandydaci do zatrudnienia	dane z cv, listów motywacyjnych, pozostałe dane z procesu rekrutacji	Zał. 13 Polityki pkt		zgodnie z klauzulą z kol. O	Polityka - pkt III.4./ Zał. 5 Polityki	zał. 3 Polityki pkt		Zał. 13 Polityki pkt	klauzula nr ...	Załącznik 12 Polityki	
2.	pracownicy	dział kadr	art. 6 ust. 1 lit. a., b., c., f.	obsługa zatrudnienia	osoby fizyczne - osoby zatrudnione	dane zgodne z art. 22.1.kp, dane pozyskiwane na podstawie zgody (nr tel., adres e-mail)			zgodnie z klauzulą z kol. O	Polityka - pkt III.4./ Zał. 5 Polityki	zał. 3 Polityki pkt		Zał. 13 Polityki pkt	klauzula nr ...	Załącznik 12 Polityki	
3.	dostawcy	dział księgowości	art. 6 ust. 1 lit. b., f.	wykonanie umowy z dostawcą	osoby fizyczne prowadzące działalność gospodarczą	dane kontaktowe (w szczególności: imię, nazwisko, firma, adres, nr tel., adres e-mail)			zgodnie z klauzulą z kol. O	Polityka - pkt III.4./ Zał. 5 Polityki	zał. 3 Polityki pkt		Zał. 13 Polityki pkt	klauzula nr ...	Załącznik 12 Polityki	
4.	klienci	dział księgowości	art. 6 ust. 1 lit. b., f.	wykonanie umowy z klientem	osoby fizyczne prowadzące działalność gospodarczą	dane kontaktowe (w szczególności: imię, nazwisko, firma, adres, nr tel., adres e-mail)			zgodnie z klauzulą z kol. O	Polityka - pkt III.4./ Zał. 5 Polityki	zał. 3 Polityki pkt		Zał. 13 Polityki pkt	klauzula nr ...	Załącznik 12 Polityki	
5.	monitoring		art. 6 ust. 1 lit. f.	zapewnienie bezpieczeństwa fizycznego	osoby, których wizerunek został utrwalony na monitoringu	wizerunek			zgodnie z klauzulą z kol. O	Polityka - pkt III.4./ Zał. 5 Polityki	zał. 3 Polityki pkt		Zał. 13 Polityki pkt	klauzula nr ...	Załącznik 12 Polityki	

ZAŁĄCZNIK NR 9

PROJEKTOWANIE/ DOMYŚLNA OCHRONA/ ANALIZA WPŁYWU

NAZWA PROCESU:		
WŁAŚCICIEL PROCESU:		
DATA WDROŻENIA PROCESU:		
DATA ROZPOCZĘCIA KONSULTACJI:		
OBSZARY WPŁYWU		
1.	Opis procesu	
2.	Kategorie osób, których dane są przetwarzane	
3.	Cel przetwarzania danych	
4.	Zakres przetwarzanych danych osobowych	
5.	Czy zakres danych jest niezbędny do osiągnięcia celu przetwarzania?	
6.	Kto będzie miał dostęp do danych osobowych?	
7.	Jak długo będą przetwarzane dane osobowe?	
8.	Podstawa prawna przetwarzania danych osobowych	
9.	Forma przetwarzania danych osobowych /system IT, papierowa/	
10.	Źródło pozyskania danych osobowych	
11.	Forma pozyskania danych osobowych	
12.	Jakie zagrożenia mogą wystąpić w odniesieniu do danych osobowych?	
13.	Na jakim etapie procesu?	
14.	Jakie zabezpieczenia w systemie IT są konieczne do zapewnienia ochrony danych osobowych?	
15.	Czy system IT wymaga dodatkowych nakładów, aby zapewnić zabezpieczenia z pkt 9.?	

16.	Czy proces wymaga opracowania i wdrożenia nowych polityk/ procedur?	
17.	Czy proces wymaga przeprowadzenia szkolenia?	
18.	Kto będzie właścicielem danych osobowych?	
19.	Jeśli dane osobowe w procesie są danymi powierzonymi przez inny podmiot, czy jest zawarta umowa powierzenia?	
20.	Czy dane będą powierzane innemu podmiotowi?	
21.	Czy dane osobowe w ramach procesu wymagają spełnienia obowiązku informacyjnego wobec osób, których dane będą przetwarzane?	
	Inne	

Uwaga!

Podczas powyższej analizy, każdorazowo, w odniesieniu do każdego procesu należy przeanalizować, zawsze z udziałem działu kadr czy nie zachodzą przesłanki do przeprowadzenia oceny skutków dla ochrony danych i obowiązek przeprowadzenia uprzednich konsultacji, w trybie art. 35 RODO.

Dla celów kontrolnych każdorazowo należy sprawdzić, publikowny przez organ nadzorczy, wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych.

ZAŁĄCZNIK NR 10

OSOBA UPOWAŻNIONA DO NADAWANIA UPOWAŻNIEŃ DO PRZTWARZANIA DANYCH OSOBOWYCH

Upoważniam Panią/ Pana …….. zatrudnioną/ zatrudnionego na stanowisku ……. w SmartQube Sp. z o. o. (zwanej dalej Spółką), będącej Administratorem danych osobowych zgodnie 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, do:

- nadawania w imieniu Spółki upoważnień do przetwarzania danych osobowych. Upoważnienie będzie następowało w formie pisemnej, na standardowym formularzu, którego wzór stanowi załącznik do Polityki ochrony danych osobowych, w oparciu o wnioski o nadanie upoważnień do przetwarzania danych osobowych, zgodnie z procedurą nadawania upoważnień określoną w Polityce ochrony danych osobowych.

Niniejsze pełnomocnictwo wygasa z chwilą ustania zatrudnienia, ponadto może zostać odwołane w każdym czasie.

Niniejsze pełnomocnictwo nie upoważnia do udzielania dalszych pełnomocnictw.

……

Podpis mocodawcy

……

Podpis osoby upoważnionej

ZAŁĄCZNIK NR 11

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Działając w imieniu SmartQube Sp. z o. o. upoważniam Panią/ Pana ...../ identyfikator ..... do przetwarzania danych osobowych, zarówno w formie papierowej, jak i w systemach informatycznych, w niżej wymienionych zbiorach danych, w zakresie i celu niezbędnym do wykonywania zadań wynikających z zatrudnienia.*

Upoważnienie dotyczy zbiorów danych:

1) ……

-zakres upoważnienia do przetwarzania danych osobowych :

- pełny zakres, zgodnie z art. 4 pkt 3 Rozporządzenia*
- ograniczony zakres przetwarzania danych osobowych**, tj. ……

2) ……

-zakres upoważnienia do przetwarzania danych osobowych :

- pełny zakres, zgodnie z art. 4 pkt 3 Rozporządzenia*
- ograniczony zakres przetwarzania danych osobowych**, tj. ……

3) ……

-zakres upoważnienia do przetwarzania danych osobowych :

- pełny zakres, zgodnie z art. 4 pkt 3 Rozporządzenia*
- ograniczony zakres przetwarzania danych osobowych**, tj. ……

n)……

-zakres upoważnienia do przetwarzania danych osobowych :

- pełny zakres, zgodnie z art. 4 pkt 3 Rozporządzenia*
- ograniczony zakres przetwarzania danych osobowych**, tj. ……

Upoważnienie ważne:

- na czas określony począwszy od _____ do _____
- na czas nieokreślony od …….

Upoważnienie to wygasa z dniem rozwiązania lub wygaśnięcia umowy będącej podstawą zatrudnienia pomiędzy osobą upoważnioną oraz Administratorem. Upoważnienie może być odwołane w każdym czasie. Osoba upoważniona jest obowiązana do zachowania w poufności przetwarzanych danych osobowych oraz sposobu ich zabezpieczenia także po ustaniu zatrudnienia.

Miejsce i data wydania upoważnienia: _____

W imieniu Administratora Osoba upoważniona

_____ _____

**zakres upoważnienia może być ograniczony zakresem nadawanych dostępów i poziomów uprawnień, realizowanych w ramach odrębnych procesów.*

**Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.*

***należy wymienić czynności przetwarzania spośród wskazanych w art. 4 pkt 2 w/w Rozporządzenia*

ZAŁĄCZNIK NR 12

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Imię i nazwisko osoby upoważnionej	Identyfikator	Data nadania upoważnienia	Data szkolenia	Data podpisania oświadczenia o zachowaniu poufności	Zakres upoważnienia	Podstawa zatrudnienia	Data ustania upoważnienia	Uwagi

ZAŁĄCZNIK NR 13

WYKAZ PODMIOTÓW, KTÓRYM ADMINISTRATOR POWIERZYŁ PRZETWARZANIE DANYCH OSOBOWYCH W TRYBIE ART. 28 RODO

Lp.	Nazwa podmiotu	Przedmiot powierzenia	Data zawarcia umowy powierzenia	Adnotacje o umowie w Rejestrze czynności przetwarzania
1	_____	Dane księgowe		
2	_____	Dane w systemach informatycznych		

ZAŁĄCZNIK NR 14

ZGŁOSZENIE INCYDENTU

Data zgłoszenia incydentu: ….
Data zidentyfikowania incydentu: ….
Data zdarzenia: ……
Imię i nazwisko, stanowisko osoby zgłaszającej: ……
Opis zdarzenia (możliwie szczegółowy): …….
Opis podjętych działań po zidentyfikowaniu incydentu: ……
Informacja o dokumentacji dotyczącej incydentu: …….

ZAŁĄCZNIK NR 15

RAPORT POSTĘPOWANIA Z INCYDENTEM

1.	Data sporządzenia raportu		
2.	Data zawiadomienia o incydencie		
3.	Forma zawiadomienia		
4.	Data zaistnienia incydentu		
5.	Osoba zgłaszająca		
6.	Opis zdarzenia		
7.	Opis działań zabezpieczających podjętych bezpośrednio po zidentyfikowaniu incydentu		
8.	Opis ustalonych przyczyn incydentu		
9.	Opis skutków incydentu		
10.	Podjęte działania korygujące i naprawcze		
11.	Zgłoszenie naruszenia do organu nadzoru		
12.	Zgłoszenie zawiadomienia do osoby, której dane dotyczą		
13.	Czy incydent spowodował konieczność informowania podmiotów trzecich innych niż organ nadzoru i osoba, której dane dotyczą		
14.	Dane osoby sporządzającej raport i podpis		
15.	Informacja o adresatach raportu		

ZAŁĄCZNIK NR 16

REJESTR INCYDENTÓW

Lp.	Incydent	Źródło i forma zgłoszenia	Data i godzina zgłosznia	Podjęte działania koryujące i osoba odpowiedzialna za wdrożenie działań, data	Podjęte działania zapobiegawcze i osoba odpowiedzialna za podjęcie działań, data	Kontrola wykonania i skuteczności podjętych działań korygujących i zapobiegawczych, osoba odpowiedzielna, data	Obowiązki notyfikacyjne w trybie art. 33 i 34 RODO	Data zamknięcia postępowania z incydentem

ZAŁĄCZNIK NR 17

REJESTR UDOSTĘPNIEŃ DANYCH OSOBOWYCH

Lp.	Osoba, której dane dotyczą	Podmiot, któremu udostępniono dane osobowe	Podstawa prawna udostępnienia danych osobowych	Data udostępnienia	Zbiór, z którego dane zostały udostępnione	Cel i zakres udostępnienia	Forma udostępnienia danych osobowych	Obowiązek informacyjny wobec osoby, której dane dotyczą

ZAŁĄCZNIK NR 18

OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI

1. Oświadczam niniejszym, że w związku z zatrudnieniem w SmartQube Sp. z o. o. przyjmuję do wiadomości, że będę przetwarzać dane osobowe i w związku z tym zobowiązuję się do przestrzegania przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, zwanego dalej RODO, zwłaszcza zobowiązuję się do ochrony powierzonych mi do przetwarzania danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Oświadczam niniejszym, że w związku z zatrudnieniem w SmartQube Sp. z o.o. zobowiązuję się do ochrony danych poufnych, niezależnie od sposobu i źródła pozyskania danych. Zobowiązuję się do ochrony danych poufnych zarówno podczas zatrudnienia jak i po ustaniu zatrudnienia. Oświadczam, że ochronę tych informacji będę traktować z najwyższą starannością i dbałość ta nigdy nie będzie mniejsza niż rozsądna.
3. Przyjmuję do wiadomości, że bezwzględnej ochronie podlegają wszystkie dane poufne SmartQube Sp. z o. o. w szczególności:
   a) Informacje o charakterze ekonomicznym, technicznym, handlowym, finansowym (w tym informacje o wynagrodzeniach).
   b) Informacje o zawartych umowach z kontrahentami.
   c) Dane osobowe.
   d) Strategia.
   e) Wdrożone środki organizacyjne, techniczne i technologiczne, system informatyczny i jego zabezpieczenia, dokumentacja systemu ochrony danych osobowych.
4. Zobowiązuję się nie ujawniać, nie kopiować, nie powielać, nie wynosić poza obszar należący do SmartQube Sp. z o.o. danych poufnych, niezależnie od ich formy ani nośnika, ani w jakikolwiek inny sposób rozpowszechniać danych poufnych, inaczej niż w związku z wykonywaniem obowiązków wynikających z zatrudnienia.
5. Jednocześnie oświadczam, że zostałam/ zostałem przeszkolony oraz że zapoznałam/ zapoznałem się z treścią i zobowiązuję się przestrzegać wszelkich procedur obowiązujących w SmartQube Sp. z o.o. dotyczących ochrony danych osobowych – w szczególności określonych w Polityce ochrony danych osobowych.
6. Oświadczam, że zostałam/ zostałem poinformowana/ poinformowany o obowiązujących w SmartQube Sp. z o. o. zasadach, dotyczących przetwarzania danych osobowych, określonych w Polityce ochrony danych osobowych i pozostałych dokumentach związanych.

7. Przyjmuję do wiadomości, że niniejsze oświadczenie obejmuje także obowiązek zaniechania czynów mających znamiona nieuczciwej konkurencji w rozumieniu Ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2009 r. Nr 201, poz. 1540, ze zm.).
8. Przyjmuję do wiadomości, że naruszenie niniejszego zobowiązania skutkować może odpowiedzialnością wynikającą z powszechnie obowiązujących przepisów prawa i ustawy o zwalczaniu nieuczciwej konkurencji.

..... *.....*

miejscowność, data *czytelny podpis osoby składającej oświadcznie*

7.