POLITYKA OCHRONY DANYCH OSOBOWYCH I BEZPIECZEŃSTWA

GHELAMCO POLAND SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

PRZYJĘTA DNIA 12 LIPCA 2021 ROKU

1. Niniejszy dokument zatytułowany „Polityka ochrony danych osobowych" (dalej jako „**Polityka**") ma za zadanie stanowić mapę wymogów, zasad i regulacji w zakresie ochrony danych osobowych w Ghelamco Poland Spółka z ograniczoną odpowiedzialnością Spółka komandytowa z siedzibą w Warszawie przy Pl. Europejskim 1, 00 844 Warszawa, wpisaną do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m. st. Warszawy w Warszawie, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000767269 (dalej jako „**Ghelamco Poland**" lub „**Spółka**").

2. Polityka jest polityką ochrony danych osobowych w rozumieniu RODO - rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L119, s. 1).

3. Biorąc pod uwagę fakt, że:

   3.1. Inne spółki z Grupy Ghelamco są powiązane kapitałowo ze Spółką;

   3.2. Inne spółki z Grupy Ghelamco stosują te same zabezpieczenia oraz zasady ochrony danych osobowych co Spółka,

   Polityka oraz załączniki do Polityki mają zastosowanie w Spółce oraz w pozostałych spółkach z Grupy Ghelamco, o ile konkretna spółka z Grupy Ghelamco nie przyjęła odrębnego dokumentu polityki ochrony danych osobowych. Polityka będzie bezpośrednio stosowana w szczególności w spółkach z Grupy Ghelamco wymienionych w załączniku nr 3 do Polityki. Wszelkie postanowienia Polityki dotyczące Spółki znajdują odpowiednie zastosowanie do pozostałych spółek z Grupy Ghelamco, do których Polityka ma zastosowanie, o ile nic innego nie wynika wyraźnie z kontekstu.

4. Odpowiedzialny za:

   4.1. wdrożenie i utrzymanie niniejszej Polityki oraz nadzór i monitorowanie jej przestrzegania jest zarząd Spółki;

   4.2. stosowanie Polityki jest Spółka i jej personel oraz inne osoby działające w imieniu Spółki;

   Spółka powinna też zapewnić zgodność postępowania kontrahentów Spółki z Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez Spółkę.

5. **Skróty i definicje:**

   5.1. „**Polityka**" oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu;

   5.2. „**RODO**" oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119.S.1);

M

5.3. „**Administrator**" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania Danych;

5.4. „**Dane**" oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu;

5.5. „**Dane wrażliwe**" oznaczają Dane specjalne i Dane karne;

5.6. „**Dane specjalne**" oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej;

5.7. „**Dane karne**" oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa;

5.8. „**Dane dzieci**" oznaczają dane osób poniżej 16. roku życia;

5.9. „**Podmiot przetwarzający**" oznacza podmiot, któremu Spółka powierzyła przetwarzanie Danych (np. usługodawca IT, zewnętrzna księgowość);

5.10. „**Profilowanie**" oznacza dowolną formę zautomatyzowanego przetwarzania Danych, 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;

5.11. „**Eksport Danych**" oznacza przekazanie Danych do państwa trzeciego lub organizacji międzynarodowej;

5.12. „**RCPD**" lub „**Rejestr**" oznacza rejestr czynności przetwarzania danych osobowych, tj. rejestr, o którym mowa w art. 30 ust. 1 RODO (rejestr dotyczący Danych, które Spółka przetwarza jako Administrator);

5.13. „**Rejestr kategorii czynności przetwarzania Danych**" oznacza rejestr, o którym mowa w art. 30 ust. 2 RODO (rejestr dotyczący Danych, które Spółka przetwarza jako Podmiot przetwarzający);

5.14. „**Spółka**" oznacza Ghelamco Poland Spółka z ograniczoną odpowiedzialnością z siedzibą w Warszawie przy Pl. Europejskim 1, 00-844 Warszawa, wpisaną do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m. st. Warszawy w Warszawie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000767269;

5.15. „**Grupa Ghelamco**" oznacza grupę kapitałową w rozumieniu ustawy o rachunkowości z dnia 29 września 1994 r. (Dz. U. z 2021 r. poz. 217), w skład której wchodzi Spółka;

5.16. „**IOD**" lub „**Inspektor**" oznacza Inspektora Ochrony Danych, osobę wyznaczoną przez Administratora, nadzorującą przestrzeganie przepisów o ochronie Danych w organizacji Administratora, wykonującą zadania określone w art. 39 RODO;

5.17. „**Ustawa**" oznacza ustawę o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz. U. z 2019 r. poz. 1781).

6. **Ochrona Danych w Spółce - zasady ogólne**

6.1. Filary ochrony Danych w Spółce:

a) **Legalność** - Spółka dba o ochronę prywatności i przetwarza Dane zgodnie z prawem;

b) **Bezpieczeństwo** - Spółka zapewnia odpowiedni poziom bezpieczeństwa Danych podejmując stale działania w tym zakresie;

c) **Prawa Jednostki** - Spółka umożliwia osobom, których Dane przetwarza, wykonywanie tych praw i prawa te realizuje;

d) **Rozliczalność** - Spółka dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność;

e) **Podejście oparte na ryzyku** – Spółka identyfikuje ryzyka towarzyszące przetwarzaniu Danych oraz ustala ich wpływ na operacje związane z Danymi, a w szczególności na prawa i wolności osób fizycznych.

6.2. Zasady ochrony Danych

Spółka przetwarza Dane z poszanowaniem następujących zasad:

a) w oparciu o podstawę prawną i zgodnie z prawem (**legalizm**);

b) rzetelnie i uczciwie (**rzetelność**);

c) w sposób przejrzysty dla osoby, której Dane dotyczą (**transparentność**);

d) w konkretnych celach i nie „na zapas" (**minimalizacja**);

e) nie więcej niż potrzeba (**adekwatność**);

f) z dbałością o prawidłowość Danych (**prawidłowość**);

g) nie dłużej niż potrzeba (**czasowość**);

h) zapewniając odpowiednie bezpieczeństwo Danych (**bezpieczeństwo**);

i) dokumentując czynności przetwarzania Danych tak, aby w każdej chwili móc wykazać zgodność działań Spółki z prawem (**rozliczalność);**

j) umożliwiając osobom, których Dane Spółka przetwarza realizację ich praw, o ile dane żądanie nie stoi w sprzeczności z obowiązującym prawem (**przestrzeganie praw jednostki**),

k) w sposób zapewniający bezpieczeństwo Danych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, poprzez wdrożenie odpowiednich środków technicznych lub organizacyjnych (**integralność i poufność**).

7. **System ochrony Danych**

System ochrony Danych w Spółce składa się z następujących elementów:

7.1. **Inwentaryzacja Danych.** Spółka dokonuje identyfikacji zasobów Danych w Spółce, w tym:

a) przypadków przetwarzania Danych specjalnych i Danych karnych (Dane wrażliwe);

b) przypadków przetwarzania Danych osób, których Spółka nie identyfikuje (dane niezidentyfikowane);

c) przypadków przetwarzania Danych dzieci;

d) Profilowania;

e) współadministrowania Danymi;

f) powierzenia przetwarzania Danych Podmiotom przetwarzającym.

7.2. **Rejestr.** Spółka opracowuje, prowadzi i utrzymuje Rejestr i Rejestr kategorii czynności przetwarzania Danych. Rejestry są narzędziami rozliczania zgodności z ochroną Danych w Spółce.

7.3. **Podstawy prawne**. Spółka identyfikuje oraz weryfikuje podstawy prawne przetwarzania Danych i rejestruje je w rejestrach, w tym:

a) utrzymuje system zarządzania zgodami na przetwarzanie Danych i komunikacją na odległość;

b) wskazuje uzasadnienie przypadków, gdy Spółka przetwarza Dane na podstawie prawnie uzasadnionego interesu Spółki.

7.4. **Zgoda.** Spółka przetwarza Dane na podstawie zgody tylko, gdy nie ma innej podstawy przetwarzania Danych oraz dba o prawidłowość przetwarzania Danych na podstawie zgody, w tym:

a) nie odbiera zgody na przetwarzanie Danych związanych z zawarciem i wykonaniem umowy lub w odniesieniu do takich Danych, których obowiązek przetwarzania wynika z przepisów prawa;

b) nie wywiera przymusu w celu uzyskania zgody;

c) formułuje zgodę w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem;

d) zapewnia, aby wycofanie zgody było równie proste jak jej złożenie.

7.5. **Obsługa praw jednostki.** Spółka spełnia obowiązki informacyjne względem osób, których Dane przetwarza oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:

a) **Obowiązki informacyjne**. Spółka przekazuje osobom prawem wymagane informacje przy zbieraniu ich Danych oraz zapewnia udokumentowanie realizacji tych obowiązków;

b) **Możliwość wykonania żądań**. Spółka weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających, z uwzględnieniem ograniczeń nakładanych na Spółkę w związku z obowiązkiem przestrzegania tajemnicy zawodowej;

c) **Obsługa żądań**. Spółka zapewnia odpowiednie procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO i udokumentowane;

d) **Zawiadamianie o naruszeniach**. Spółka stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem Danych.

e) **Minimalizacja.** Spółka zarządza minimalizacją (privacy by default), a w tym:

i. adekwatnością Danych;

ii. reglamentacją i zarządzaniem dostępem do Danych;

iii. okresem przechowywania Danych i weryfikacji dalszej przydatności.

f) **Bezpieczeństwo.** Spółka zapewnia wysoki poziom bezpieczeństwa Danych, w tym:

i. przeprowadza analizy ryzyka dla czynności przetwarzania Danych lub ich kategorii;

ii. przeprowadza oceny skutków dla ochrony Danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;

iii. dostosowuje środki ochrony Danych do ustalonego ryzyka;

iv. stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony Danych Prezesowi Urzędu Ochrony Danych;

v. zarządza incydentami.

g) **Podmiot przetwarzający.** Spółka stosuje kryteria doboru Podmiotów przetwarzających Dane na rzecz Spółki, wymogi co do warunków przetwarzania (umowa powierzenia), kryteria weryfikacji wykonywania umów powierzenia.

h) **Eksport Danych.** Spółka weryfikuje, czy Spółka nie przekazuje Danych do państw trzecich (czyli poza UE, Norwegię, Lichtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnia zgodne z prawem warunki takiego przekazywania, jeśli ma ono miejsce.

Dodatkowo, Spółka:

i. kontroluje czy przekazuje jakiekolwiek Dane do państw trzecich lub organizacji międzynarodowych, w szczególności w przypadku, gdy korzysta z usług innego podmiotu;

ii. identyfikuje i weryfikuje podstawę prawną przekazywania Danych do państw trzecich lub organizacji międzynarodowych;

iii. odnotowuje w prowadzonych rejestrach przypadki przekazywania Danych do państw trzecich lub organizacji międzynarodowych.

i) **Privacy by design.** Spółka zarządza zmianami mającymi wpływ na prywatność. W tym celu przy uruchamianiu nowych projektów i inwestycji w Spółce uwzględnia się konieczność oceny wpływu zmiany na ochronę Danych, zapewnienie prywatności (a w tym celu zgodności celów przetwarzania, bezpieczeństwa Danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.

j) **Przetwarzanie transgraniczne.** Spółka weryfikuje, kiedy zachodzą przypadki przetwarzania transgranicznego oraz ustala wiodący organ nadzorczy i główną jednostkę organizacyjną w rozumieniu RODO.

8. **Inwentaryzacja**

8.1. Dane wrażliwe

Spółka identyfikuje przypadki, w których przetwarza lub może przetwarzać Dane wrażliwe (Dane specjalne i Dane karne) oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania Danych wrażliwych. W przypadku zidentyfikowania przypadków przetwarzania Danych wrażliwych, Spółka postępuje zgodnie z przyjętymi zasadami w tym zakresie.

8.2. Dane niezidentyfikowane

Spółka identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane.

8.3. Profilowanie

Spółka identyfikuje przypadki, w których dokonuje Profilowania przetwarzania Danych i utrzymuje mechanizmy zapewniające zgodność tego procesu z prawem. W przypadku zidentyfikowania przypadków Profilowania i zautomatyzowanego podejmowania decyzji, Spółka postępuje zgodnie z przyjętymi zasadami w tym zakresie.

8.4. Współadministrowanie

Spółka identyfikuje przypadki współadministrowania Danymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami. RCPD uwzględnia wyniki wykonywanej w Spółce inwentaryzacji Danych.

9. **Rejestr czynności przetwarzania Danych**

9.1. RCPD stanowi formę dokumentowania czynności przetwarzania Danych, pełni rolę mapy przetwarzania Danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony Danych, czyli zasady rozliczalności.

9.2. Spółka prowadzi Rejestr, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje Dane.

9.3. Rejestr jest jednym z podstawowych narzędzi umożliwiających Spółce rozliczanie większości obowiązków ochrony Danych.

9.4. W Rejestrze, dla każdej czynności przetwarzania Danych, którą Spółka uznała za odrębną dla potrzeb Rejestru, Spółka odnotowuje co najmniej: (i) nazwę czynności, (ii) cel przetwarzania, (iii) opis kategorii osób, (iv) opis kategorii Danych, (v) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu Spółki, jeśli podstawą jest uzasadniony interes, (vi) sposób zbierania Danych, (vii) opis kategorii odbiorców Danych (w tym Podmiotów przetwarzających), (viii) informację o przekazaniu poza EU/EOG; (ix) ogólny opis technicznych i organizacyjnych środków ochrony Danych.

10. **Rejestr kategorii czynności przetwarzania Danych**

10.1. Rejestr kategorii czynności przetwarzania stanowi formę dokumentowania i inwentaryzacji czynności przetwarzania Danych, które Spółka przetwarza jako podmiot przetwarzający, tj. w imieniu innych Administratorów, pełni rolę mapy przetwarzania tych Danych i jest jednym z elementów umożliwiających realizację zasady rozliczalności.

10.2. Spółka prowadzi Rejestr kategorii czynności przetwarzania, w którym inwentaryzuje i

monitoruje sposób, w jaki wykorzystuje Dane przetwarzane jako podmiot przetwarzający.

10.3. W rejestrze, dla każdej kategorii czynności przetwarzania Danych (przetwarzanych jako podmiot przetwarzający), którą Spółka uznała za odrębną dla potrzeb tego rejestru, Spółka odnotowuje co najmniej:

a) nazwę kategorii czynności przetwarzania;

b) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa;

c) dane Administratora, w imieniu którego Spółka działa jako podmiot przetwarzający;

d) czas przetwarzania;

e) czy przekazuje Dane do państwa trzeciego lub organizacji międzynarodowej;

f) dane podmiotów podprzetwarzających.

11. **Inspektor Ochrony Danych**

11.1. Decyzja o powołaniu IOD należy do Spółki, która biorąc pod uwagę konieczność zapewnienia rozliczalności w zakresie przestrzegania ochrony Danych oraz spełnienia wymogów wynikających z RODO, ma prawny obowiązek powołania IOD, bądź możliwość powołania IOD. Postanowienia dotyczące IOD określone w Polityce stosuje się pod warunkiem powołania IOD przez Spółkę.

11.2. IOD może zostać wyłącznie osoba, która posiada fachową wiedzę na temat prawa i praktyki w ochronie Danych; IOD nie musi być pracownikiem Spółki.

11.3. W przypadku powołania IOD Spółka jest zobowiązana do udostępnienia danych kontaktowych IOD oraz do zawiadomienia o powołaniu IOD organu nadzorczego.

11.4. Status prawny i zadania IOD regulują przepisy rozdziału IV Sekcji 4 RODO.

11.5. IOD w wykonywaniu swoich zadań podlega bezpośrednio zarządowi Spółki.

11.6. Do zadań IOD należy w szczególności:

a) informowanie zarządu Spółki oraz pracowników/współpracowników Spółki, którzy przetwarzają Dane o obowiązkach wynikających z RODO oraz innych przepisów Unii Europejskiej lub państw członkowskich o ochronie Danych i doradzanie im w zakresie ww. obowiązków;

b) monitorowanie przestrzegania RODO, innych przepisów dotyczących ochrony Danych osobowych oraz prowadzenie szkoleń wewnętrznych zwiększających świadomość pracowników/współpracowników Spółki w zakresie zasad dotyczących ochrony Danych;

c) pełnienie funkcji punktu kontaktowego dla właściwych organów i podmiotów zewnętrznych w kwestiach związanych z przetwarzaniem przez Spółkę Danych;

d) podejmowanie działań zwiększających świadomość w zakresie ochrony Danych, w tym szkoleń personelu uczestniczącego w operacjach przetwarzania oraz prowadzenie powiązanych z tym audytów;

e) udzielanie, na żądanie, zaleceń co do oceny skutków dla ochrony Danych oraz monitorowania jej wykonania zgodnie z art.35 RODO;

f) współpraca z organem nadzorczym.

h

11.7. Spółka jest zobowiązana zapewnić, by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony Danych.

11.8. Spółka jest zobowiązana wspierać IOD w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do Danych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.

11.9. Spółka jest zobowiązana do zapewnienia IOD warunków niezbędnych do niezależnego i skutecznego wykonywania zadań i w tym zakresie w szczególności:

a) nie może wydawać IOD żadnych instrukcji dotyczących wykonywania przez niego zadań;

b) nie może karać IOD za wykonywanie przez niego obowiązków, o ile są one wykonywane w sposób należyty i zgodny z prawem;

c) nie może odwołać IOD za wykonywanie przez niego obowiązków, o ile są one wykonywane w sposób należyty i zgodny z prawem.

11.10. Spółka przy działaniu oraz podejmowaniu decyzji powinna zawsze brać pod uwagę stanowisko IOD, zaś wszelkie przypadki postępowania niezgodnego z zaleceniami przekazanymi przez IOD powinny być dokumentowane wraz ze wskazaniem powodów przyjęcia odmiennych rozwiązań.

12. Osoby Upoważnione

12.1. Przetwarzania Danych w ramach struktury Spółki mogą dokonywać wyłącznie osoby upoważnione przez Spółkę. Spółka upoważnia osoby do przetwarzania Danych.

12.2. Każda osoba, a w szczególności osoba, która otrzymała upoważnienie do przetwarzania Danych, zobowiązana jest do ich ochrony w sposób zgodny z przepisami RODO, innymi aktami prawnymi obowiązującymi w polskim systemie prawnym oraz Polityką i dokumentami wdrożonymi w Spółce zgodnie z przepisami RODO.

12.3. Spółka zapewnia, aby żadna z osób upoważnionych nie miała dostępu do większej ilości Danych i procesów przetwarzania Danych niż jest to konieczne do prawidłowego wypełniania przez nią jej obowiązków i zadań.

12.4. Spółka zapewnia osobom upoważnionym dostęp do dokumentów z zakresu ochrony Danych, z wyjątkiem tych dokumentów, które nie powinny być dostępne dla wszystkich osób upoważnionych.

12.5. Spółka prowadzi ewidencję osób upoważnionych do przetwarzania Danych.

12.6. Osoby upoważnione przetwarzające Dane są zobowiązane w szczególności do:

a) przetwarzania Danych zgodnie z posiadanym upoważnieniem oraz z należytą starannością;

b) w przypadku zaobserwowania zdarzenia mogącego stanowić naruszenie ochrony Danych niezwłocznego informowania o nim bezpośredniego przełożonego oraz IOD;

c) uczestnictwa w organizowanych szkoleniach z zakresu ochrony Danych;

d) zachowania poufności Danych oraz informacji na temat sposobu ich zabezpieczenia, zgodnie z zasadą poufności.

13. **Odbiorcy Danych**

13.1. Spółka może udostępniać Dane podmiotom trzecim wyłącznie:

a) w realizacji celów ze względu na które Spółka Dane przetwarza i w ramach właściwych podstaw prawnych przetwarzania Danych – na mocy stosownego upoważnienia lub umowy powierzenia przetwarzania Danych albo

b) na podstawie obowiązujących przepisów - podmiotom upoważnionym na podstawie przepisów prawa (np. sądom, organom ścigania itp.).

13.2. W przypadku braku podstawy prawnej, Spółka odmawia udostępnienia Danych jakiemukolwiek odbiorcy.

13.3. Kategorie odbiorców Danych wskazywane są w Rejestrze, a także w klauzulach informacyjnych przekazywanych osobom, których Dane Spółka przetwarza.

14. **Podstawy przetwarzania**

14.1. Spółka przetwarza Dane wyłącznie, gdy ma do tego jedną z podstaw prawnych określonych w art. 6 ust. 1 RODO lub w art. 9 ust. 2 RODO. Gdy Spółka przetwarza Dane jako Podmiot przetwarzający, zobowiązuje w umowach Administratorów tych Danych, żeby Dane, które powierzają Spółce były Danymi przetwarzanymi przez nich na właściwej podstawie prawnej.

14.2. Spółka dokumentuje w Rejestrze podstawy prawne przetwarzania Danych dla poszczególnych czynności przetwarzania.

14.3. Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel Spółki), Spółka dookreśla podstawę w czytelny sposób, gdy jest to potrzebne, np. dla zgody – wskazując na jej zakres, gdy podstawą jest prawo – wskazując na konkretny przepis i inne dokumenty, np. umowę, porozumienie administracyjne, żywotne interesy – wskazując na kategorie zdarzeń, w których się zmaterializują, uzasadniony cel – wskazując na konkretny cel, np. marketing własny, dochodzenie roszczeń.

14.4. Spółka wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych Danych w konkretnym celu, zgody na komunikację na odległość (email, telefon, sms, in.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie, itp.).

15. **Sposób obsługi praw jednostki i obowiązków informacyjnych**

15.1. Spółka dba o czytelność i styl przekazywania informacji i komunikacji z osobami, których Dane przetwarza.

15.2. Spółka ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczenie na stronie internetowej Spółki informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich w Spółce, w tym wymaganiach dotyczących identyfikacji, metodach kontaktu ze Spółką w tym celu, ewentualnym cenniku żądań „dodatkowych" itp.

15.3. Spółka dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.

15.4. Spółka wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.

15.5. W celu realizacji praw jednostki Spółka zapewnia procedury i mechanizmy pozwalające

zidentyfikować Dane konkretnych osób przetwarzane przez Spółkę, wprowadzać do nich zmiany i usuwać w sposób zintegrowany.

15.6. Spółka dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

16. **Obowiązki informacyjne**

16.1. Spółka określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.

16.2. Spółka informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.

16.3. Spółka informuje osobę o przetwarzaniu jej Danych, przy pozyskiwaniu Danych od tej osoby.

16.4. Spółka informuje osobę o przetwarzaniu jej Danych, przy pozyskiwaniu Danych o tej osobie niebezpośrednio od niej (chyba, że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).

16.5. Jeżeli przetwarzane w Spółce Dane, zbierane są od osoby, której te Dane dotyczą, Spółka realizuje wobec niej obowiązek informacyjny w zakresie określonym w art. 13 RODO.

16.6. Jeżeli przetwarzanych w Spółce Danych nie pozyskano od osoby, której Dane dotyczą, Spółka realizuje wobec tej osoby obowiązek informacyjny w zakresie określonym w art. 14 RODO.

16.7. Spółka nie jest zobowiązana do realizacji obowiązku informacyjnego w zakresie w jakim:

a) osoba, której Dane dotyczą, dysponuje już tymi informacjami;

b) udzielenie takich informacji jest niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku lub o ile wykonanie obowiązku informacyjnego może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. W takich przypadkach Spółka podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, w tym udostępnia informacje publicznie;

c) pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii Europejskiej lub prawem polskim;

d) Dane muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii Europejskiej lub w prawie polskim, w tym ustawowym obowiązkiem zachowania tajemnicy.

16.8. Spółka określa sposób informowania osób o przetwarzaniu Danych niezidentyfikowanych, tam gdzie jest to możliwe (np. stopka maila, klauzule umowne, tabliczka o objęciu obszaru monitoringiem wizyjnym).

16.9. Spółka informuje osobę o planowanej zmianie celu przetwarzania Danych.

16.10. Spółka informuje osobę przed uchyleniem ograniczenia przetwarzania (w sytuacjach wskazanych w punkcie 16.9 poniżej).

16.11. Spółka informuje odbiorców Danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania Danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).

16.12. Spółka informuje osobę o prawie sprzeciwu względem przetwarzania Danych najpóźniej przy pierwszym kontakcie z tą osobą.

16.13. Spółka bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony Danych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

17. **Żądania osób**

17.1. **Prawa osób trzecich**. Realizując prawa osób, których Dane dotyczą, Spółka wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii Danych lub prawa do przeniesienia Danych może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną Danych innych osób, prawa własności intelektualnej, tajemnicę handlową, dobra osobiste, itp.), Spółka może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia takiemu żądaniu.

17.2. **Nieprzetwarzanie.** Spółka informuje osobę o tym, że nie przetwarza Danych jej dotyczących, jeśli taka osoba zgłosi żądanie dotyczące jej praw.

17.3. **Odmowa.** Spółka informuje osobę, w terminie miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.

17.4. **Dostęp do Danych.** Na żądanie osoby dotyczące dostępu do jej Danych, Spółka informuje osobę, czy przetwarza jej Dane oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu Danych), a także udziela osobie dostępu do Danych jej dotyczących. Dostęp do Danych może być zrealizowany przez wydanie kopii Danych.

17.5. **Kopie danych.** Na żądanie Spółka wydaje osobie nieodpłatnie pierwszą kopię Danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii Danych. Spółka pobiera opłaty za kolejne kopie Danych. Cena kopii Danych skalkulowana będzie w oparciu o oszacowany jednostkowy koszt obsługi żądania wydania kopii Danych.

17.6. **Sprostowanie Danych.** Spółka dokonuje sprostowania nieprawidłowych Danych na żądanie osoby. Spółka ma prawo odmówić sprostowania Danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości Danych, których sprostowania się domaga. W przypadku sprostowania Danych Spółka informuje osobę o odbiorcach Danych, na żądanie tej osoby.

17.7. **Uzupełnienie Danych.** Spółka uzupełnia i aktualizuje Dane na żądanie osoby. Spółka ma prawo odmówić uzupełnienia Danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania Danych (np. Spółka nie musi przetwarzać Danych, które są Spółce zbędne). Spółka może polegać na oświadczeniu osoby, co do uzupełnianych Danych, chyba że będzie to niewystarczające w świetle przyjętych przez Spółkę procedur (np. co do pozyskiwania takich Danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

17.8. **Usunięcie Danych**. Na żądanie osoby, Spółka usuwa Dane, gdy:

a) Dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach;

b) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania;

c) osoba wniosła skuteczny sprzeciw względem przetwarzania tych Danych;

d) Dane były przetwarzane niezgodnie z prawem;

e) konieczność usunięcia wynika z obowiązku prawnego;

f) żądanie dotyczy Danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. profil dziecka na portalu społecznościowym, udział w konkursie na stronie internetowej).

Spółka określa sposób obsługi prawa do usunięcia Danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony Danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17 ust. 3 RODO.

Jeżeli Dane podlegające usunięciu zostały upublicznione przez Spółkę, Spółka podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te Dane, o potrzebie usunięcia Danych i dostępu do nich.

W przypadku usunięcia Danych Spółka informuje osobę o odbiorcach Danych, na żądanie tej osoby.

17.9. **Ograniczenie przetwarzania**. Spółka dokonuje ograniczenia przetwarzania Danych na żądanie osoby, gdy:

a) osoba kwestionuje prawidłowość Danych - na okres pozwalający sprawdzić ich prawidłowość;

b) przetwarzanie jest niezgodne z prawem, a osoba, której Dane dotyczą, sprzeciwia się usunięciu Danych, żądając w zamian ograniczenia ich wykorzystywania;

c) Spółka nie potrzebuje już Danych, ale są one potrzebne osobie, której Dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;

d) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją - do czasu stwierdzenia, czy po stronie Spółki zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

W trakcie ograniczenia przetwarzania Spółka przechowuje Dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której Dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.

Spółka informuje osobę przed uchyleniem ograniczenia przetwarzania.

W przypadku ograniczenia przetwarzania Danych Spółka informuje osobę o odbiorcach Danych, na żądanie tej osoby.

17.10. **Przenoszenie Danych**. Na żądanie osoby, której Dane dotyczą, Spółka wydaje w ustrukturyzowanym, powszechnie używanym formacie elektronicznym, innemu podmiotowi, jeśli jest to możliwe, Dane dotyczące tej osoby, które dostarczyła ona Spółce, a które są przetwarzane w systemie informatycznym Spółki.

17.11. **Sprzeciw w szczególnej sytuacji.** Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej Danych, a Dane przetwarzane są przez Spółkę w oparciu o uzasadniony interes Spółki lub o powierzone Spółce zadanie w interesie publicznym, Spółka uwzględni sprzeciw, o ile nie zachodzą po stronie Spółki ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

17.12. **Sprzeciw względem marketingu bezpośredniego.** Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej Danych przez Spółkę na potrzeby marketingu bezpośredniego (w tym ewentualnie Profilowanie), Spółka uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

17.13. **Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu.** Jeżeli Spółka przetwarza Dane w sposób automatyczny, w tym w szczególności profiluje osoby, i w konsekwencji podejmuje względem osoby decyzje wywołujące skutki prawne lub inaczej istotnie wpływające na osobę, Spółka zapewnia możliwość odwołania się do interwencji i decyzji człowieka po stronie Spółki, chyba że taka automatyczna decyzja (i) jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a Spółką; lub (ii) jest wprost dozwolona przepisami prawa; lub (iii) opiera się o wyraźną zgodę odwołującej się osoby;

17.14. **Kontakty z osobą, której Dane są przetwarzane przez Spółkę**

a) Spółka wdraża odpowiednie środki, aby komunikacja z osobą odbywała się w zwięzłej, przejrzystej i łatwo dostępnej formie, jasnym i prostym językiem.

b) Spółka udziela osobom informacji na piśmie lub w inny sposób, w tym w stosownych przypadkach - elektronicznie. Jeżeli osoba tego zażąda, Spółka udziela informacji ustnie, o ile jest możliwe potwierdzenie tożsamości osoby innymi sposobami.

c) Spółka ułatwia osobom wykonywanie praw przysługujących im na gruncie RODO, w tym uprawnień przewidzianych w art. 15-22 RODO.

d) Spółka bez zbędnej zwłoki udziela osobom informacji o działaniach podjętych w związku z żądaniem zgłoszonym na podstawie art. 15-22 RODO.

18. Minimalizacja

Spółka dba o minimalizację przetwarzania Danych pod kątem: (i) adekwatności Danych do celów (ilości Danych i zakresu przetwarzania), (ii) dostępu do Danych, (iii) czasu przechowywania Danych.

18.1. Minimalizacja zakresu

a) Spółka zweryfikowała zakres pozyskiwanych Danych, zakres ich przetwarzania i ilość przetwarzanych Danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO.

b) Spółka dokonuje okresowego przeglądu ilości przetwarzanych Danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.

c) Spółka przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania Danych w ramach procedur zarządzania zmianą (privacy by design).

18.2. Minimalizacja dostępu

a) Spółka stosuje ograniczenia dostępu do Danych: prawne (zobowiązania do poufności, zakresy upoważnień), fizyczne (zamykanie pomieszczeń) i logiczne (ograniczenia uprawnień do systemów przetwarzających Dane i zasobów sieciowych, w których rezydują Dane).

b) Spółka dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach Podmiotów przetwarzających.

c) Spółka dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.

18.3. Minimalizacja czasu

a) Spółka regularnie dokonuje przeglądu przetwarzanych Danych w Spółce w celu usuwania Danych, które przestają być niezbędne dla celów, do których zostały pozyskane, w tym dokonuje weryfikacji dalszej przydatności Danych względem terminów i punktów kontrolnych wskazanych w Rejestrze.

b) Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów informatycznych Spółki, jak też z akt, przechowywanych w wersji papierowej. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Spółkę. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystywania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia Danych, a w tym wymogi usuwania Danych.

19. **Bezpieczeństwo**

19.1. Spółka zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania Danych przez Spółkę.

19.2. Spółka zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania - wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.

19.3. Spółka kategoryzuje Dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.

19.4. Spółka przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania Danych lub ich kategorii. Spółka analizuje możliwe sytuacje i scenariusze naruszenia ochrony Danych, uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

19.5. Spółka dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony Danych tam, gdzie zgodnie z analizą ryzyka, ryzyko naruszenia praw i wolności osób jest wysokie

19.6. Spółka ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym Spółka ustala przydatność i stosuje takie środki i podejście jak:

a) zabezpieczanie plików zawierających zbiory Danych hasłami dostępu;

b) inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania (poprzez stosowanie takich narzędzi jak programy antywirusowe, hasłowanie, szyfrowanie, ograniczanie i monitorowanie dostępu do systemów informatycznych itp.);

c) środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności Danych i dostępu do nich w razie incydentu fizycznego lub technicznego.

19.7. Środki bezpieczeństwa

a) ograniczenie dostępu pracownika lub osoby świadczącej usługi do minimalnego zakresu Danych;

b) regularne usuwanie ze sprzętu komputerowego i nośników pamięci Danych;

c) dostęp to Internetu podlega kontroli i filtrowaniu adresów potencjalnie niebezpiecznych

d) zakaz korzystania z niezabezpieczonych zewnętrznych sieci z dostępem do Internetu bez aktywnego połączenia VPN;

e) zakaz udzielania dostępu do sprzętu komputerowego i nośników pamięci przez osoby postronne;

f) obowiązek spoczywający na pracowniku lub osobie świadczącej usługi w zakresie zabezpieczenia hasłem używanego sprzętu komputerowego i nośników pamięci;

g) obowiązek stosowania zabezpieczeń sprzętu komputerowego i nośników pamięci hasłem o wysokim stopniu złożoności; cykliczna zmiana hasła dostępu do sprzętu komputerowego i nośników pamięci;

h) zakaz wynoszenia poza teren zakładu pracy niezabezpieczonego sprzętu komputerowego i nośników pamięci;

i) obowiązek natychmiastowego zgłaszania przełożonym bądź IOD wszelkich sytuacji mogących wpływać na zabezpieczenie Danych;

j) zasada pozostawiania "czystego biurka" po zakończeniu pracy;

k) obecność osób postronnych w pomieszczeniach Spółki ograniczona tylko do osób zaproszonych;

l) nałożenie na osoby mające upoważnienie do przetwarzania Danych obowiązku bezzwłocznego powiadomienia IOD bądź przełożonego o każdym zdarzeniu zagrażającym utratą ochrony Danych oraz mogącym mieć wpływ na bezpieczeństwo Danych;

m) zamontowanie zamków elektromagnetycznych otwieranych za pomocą kart (każda osoba upoważniona będzie miała indywidualnie przypisaną kartę dostępu do wybranych pomieszczeń);

n) zwalnianie wydruku na drukarkach w pomieszczeniach ogólnodostępnych poprzez przyłożenie indywidualnie przypisanej karty;

o) zabezpieczenie pomieszczenia we właściwy sposób przed włamaniem – Dane przechowywane w specjalnych zamykanych szafach;

p) instrukcja przeciwpożarowa dla budynków, w których znajdują się Dane

q) tworzenie repliki baz Danych na serwerach, znajdujących się w oddzielnych lokalizacjach. W razie ewentualnego zdarzenia na serwerze głównym, serwer zapasowy gwarantuje dostęp do wszystkich Danych zapisanych w bazie Danych;

r) planowanie z wyprzedzeniem, w godzinach o najniższym nasileniu dostępu do systemu przez użytkowników, prac konserwacyjno-serwisowych;

h

s) informacja o planowanych pracach konserwacyjno-serwisowych z możliwie długim wyprzedzeniem.

19.8. Zgłaszanie naruszeń

Spółka stosuje procedury pozwalające na identyfikację ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony Danych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia.

19.9. Spółka opracowała i stosuje Instrukcję postępowania w procesach przetwarzania danych osobowych, stanowiącą załącznik do Polityki, która obowiązuje od 12 lipca 2021 roku.

20. Podmiot przetwarzający

20.1. Spółka może powierzyć przetwarzanie Danych Podmiotowi przetwarzającemu w zależności od własnych potrzeb.

20.2. Spółka jest zobowiązana powierzać przetwarzanie Danych tylko takim Podmiotom przetwarzającym, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których te Dane dotyczą. Zakazane jest korzystanie z usług Podmiotów przetwarzających, które takich gwarancji nie dają.

20.3. Spółka posiada zasady doboru i weryfikacji Podmiotów przetwarzających Dane na rzecz Spółki opracowane w celu zapewnienia, aby dawali oni wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony Danych spoczywających na Spółce. Spółka dokonuje weryfikacji Podmiotu przetwarzającego Dane według procedury weryfikacji podmiotu przetwarzającego Dane stanowiącej załącznik nr 2 do Polityki. Spółka, zawierając umowę o powierzeniu przetwarzania danych osobowych, dokonuje doboru i weryfikacji przetwarzających w celu zapewnienia, aby przetwarzający dawali wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na Spółce.

20.4. Każda umowa powierzenia przetwarzania Danych zawierana przez Spółkę powinna spełniać wymagania określone w RODO.

20.5. Spółka rozlicza Podmioty przetwarzające z wykorzystania podprzetwarzających, jak też z innych wymagań wynikających z zasad powierzenia Danych.

21. Spółka jako Podmiot przetwarzający

21.1. W związku z prowadzoną działalnością Spółka może być Podmiotem przetwarzającym dla innego Administratora lub innego Podmiotu Przetwarzającego. Spółka zawiera wtedy powierzenia przetwarzania Danych zgodną z art. 28 RODO.

21.2. Spółka jest zobowiązana zapewnić wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa Osób, których Dane dotyczą.

21.3. Spółka jest zobowiązana wywiązać się z obowiązków przewidzianych w umowie powierzenia przetwarzania Danych, którą zawiera z innym Administratorem Danych.

21.4. W przypadku zawarcia przez Spółkę umowy powierzenia przetwarzania Danych, Spółka prowadzi Rejestr kategorii czynności przetwarzania Danych.

22. **Eksport Danych**

22.1. Spółka rejestruje w Rejestrze przypadki Eksportu Danych, czyli przekazywania Danych poza Europejski Obszar Gospodarczy (EOG w 2021 r. = Unia Europejska, Islandia, Lichtenstein i Norwegia).

22.2. W Spółce obowiązuje zakaz korzystania z publicznie dostępnych usług chmurowych (shadow IT), aby uniknąć sytuacji nieautoryzowanego Eksportu Danych. Spółka okresowo weryfikuje zachowanie użytkowników oraz w miarę możliwości udostępnia zgodne z prawem ochrony Danych rozwiązania równoważne.

22.3. Spółka odnotowuje w Rejestrze i w rejestrze kategorii czynności przetwarzania Danych przypadki Eksportu Danych dla poszczególnych czynności przetwarzania Danych i dla poszczególnych kategorii przetwarzania Danych.

22.4. Spółka przekazuje Dane do państwa trzeciego tylko wtedy, gdy jest to konieczne i z zapewnieniem odpowiedniego stopnia ochrony, przede wszystkim poprzez:

a) współpracę z podmiotami przetwarzającymi Dane w państwach, w odniesieniu, do których została wydana stosowna decyzja Komisji Europejskiej dotycząca stwierdzenia zapewnienia odpowiedniego stopnia ochrony Danych;

b) stosowanie standardowych klauzul umownych wydanych przez Komisję Europejską;

23. **Projektowanie prywatności**

23.1. Spółka reaguje w odpowiedni sposób na zmiany np. w zakresie postępu technologii mające wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa Danych oraz minimalizacji ich przetwarzania.

23.2. W tym celu projekty i inwestycje prowadzone przez Spółkę realizowane są według zasad bezpieczeństwa Danych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę Danych, uwzględnienia i zaprojektowania bezpieczeństwa i minimalizacji przetwarzania Danych od początku projektu lub inwestycji.

24. **Nadzór i kontrola**

24.1. Niezależnie od czynności, które zostały przewidziane przez RODO dla IOD, nadzór i kontrolę nad ochroną Danych przetwarzanych w strukturze Spółki sprawuje zarząd Spółki.

24.2. W celu przeprowadzenia audytu, Spółka wyznacza audytora/ zespół audytorów lub zleca przeprowadzenie audytu firmie zewnętrznej.

24.3. Kontrolą, o której mowa powyżej, objęte są wszystkie jednostki organizacyjne, i wyodrębnione w strukturze Spółki, w których przetwarzane są Dane.

24.4. Kontrola zostaje przeprowadzana w celu ustalenia, czy nie występują Dane, które powinny zostać poddane zasadom ochrony przewidzianym przez RODO, ustawodawstwu krajowemu oraz wewnętrznej dokumentacji przetwarzania Danych, oraz w zakresie prawidłowości stosowania zasad ochrony Danych wynikających z Polityki i dokumentów wprowadzonych zgodnie z RODO.

24.5. Kontrola ma za zadanie weryfikację poprawności merytorycznej wewnętrznych regulacji z zakresu ochrony Danych, ich aktualności w odniesieniu do przepisów prawa oraz w celu ich aktualizacji w związku z przeprowadzoną analizą ryzyka oraz jej wynikami.

25. Zasady odpowiedzialności za wykonanie i naruszenie Polityki

25.1. Spółka zapewnia zgodność przetwarzania Danych z regulacjami RODO oraz krajowymi przepisami dotyczącymi ochrony Danych, tj. Ustawą, a także wytycznymi wydawanymi przez właściwe organy unijne i krajowe.

25.2. Odpowiedzialny za wdrożenie i utrzymanie Polityki jest:

a) zarząd Spółki, a w ramach zarządu - członek zarządu, któremu powierzono nadzór nad obszarem ochrony Danych;

b) osoba wyznaczona przez zarząd do zapewnienia zgodności z ochroną Danych.

25.3. Za nadzór i monitorowanie przestrzegania Polityki odpowiadają:

a) IOD;

b) komórka audytu wewnętrznego, jeżeli funkcjonuje w Spółce.

25.4. Za stosowanie Polityki odpowiedzialni są:

a) Spółka;

b) komórka organizacyjna odpowiedzialna za obszar bezpieczeństwa informacji;

c) komórki organizacyjne przetwarzające Dane;

d) wszyscy członkowie personelu Spółki.

25.5. Spółka powinna zapewnić zgodność postępowania kontrahentów Spółki z Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im Danych przez Spółkę.

25.6. Polityka dotyczy wszystkich Danych przetwarzanych bez względu na formę ich przetwarzania (przetwarzanie tradycyjne, zbiory ewidencyjne, systemy informatyczne).

25.7. Polityka jest dostępna dla wszystkich pracowników i współpracowników Spółki. Polityka powinna być dostępna w wersji elektronicznej oraz w wersji papierowej w siedzibie Spółki dla wszystkich pracowników i współpracowników Spółki.

25.8. Polityka jest udostępniana podmiotom, którym ma zostać nadane upoważnienie do przetwarzania Danych w celu zapoznania się z jej treścią.

25.9. Dla skutecznej realizacji Polityki Spółka zapewnia:

a) środki techniczne i rozwiązania organizacyjne, odpowiednie do zagrożeń i kategorii Danych objętych ochroną;

b) kontrolę i nadzór nad przetwarzaniem Danych;

c) nadzorowanie zastosowanych środków ochrony.

25.10. Nadzór przez Spółkę zastosowanych środków ochrony jest realizowany poprzez monitorowanie m.in. naruszania zasad dostępu do Danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.

25.11. Spółka zapewnia, że czynności wykonywane w związku z przetwarzaniem i zabezpieczeniem Danych są zgodne z Polityką oraz odpowiednimi przepisami prawa

26. Postanowienia końcowe

26.1. W sprawach nieuregulowanych w Polityce stosuje się powszechnie obowiązujące przepisy prawa, w tym w szczególności przepisy RODO.

26.2. Polityka została sporządzona w formie pisemnej w jednym egzemplarzu. Podpisany oryginał Polityki przechowywany jest w Spółce, natomiast jego skan/kopia jest udostępniony osobom upoważnionym przez Spółkę. Polityka wchodzi w życie z dniem 12 lipca 2021 r.

26.3. Polityka obowiązuje do czasu jej zmiany lub uchylenia. W razie potrzeby, Spółka dokonuje przeglądu Polityki, uwzględniając w szczególności analizę skutków jej obowiązywania dla ochrony Danych oraz ochrony praw i wolności osób, których te Dane dotyczą. Spółka dokona zmiany Polityki w szczególności w przypadku, gdy zmianie ulegną obowiązujące regulacje prawne w zakresie ochrony Danych.

26.4. Załącznik nr 1 do Polityki – Instrukcja postępowania w procesach przetwarzania danych osobowych, załącznik nr 2 do Polityki – Procedura weryfikacji podmiotu przetwarzającego dane osobowe oraz załącznik nr 3 – Lista spółek z Grupy Ghelamco – stanowią jej integralną część.

Warszawa, dnia 12 lipca 2021 roku

Jeroen van der Toolen

Członek Zarządu

INSTRUKCJA POSTĘPOWANIA W PROCESACH PRZETWARZANIA DANYCH OSOBOWYCH W GHELAMCO POLAND SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

Niniejsza Instrukcja określa sposób zarządzania Systemami informatycznymi wykorzystywanymi przy Przetwarzaniu Danych Osobowych u Administratora i została opracowana na podstawie Ustawy oraz RODO.

Niniejsza Instrukcja stanowi załącznik do Polityki Ochrony Danych Osobowych (dalej: „**Polityka**") obowiązującej w Ghelamco Poland sp. z o. o. Pojęcia niezdefiniowane inaczej w niniejszej instrukcji mają znaczenie nadane im w Polityce.

Nadzór nad zarządzaniem Systemem informatycznym służącym do Przetwarzania Danych Osobowych wykonuje zarząd Administratora.

§1

DEFINICJE

Zastosowane w niniejszej Instrukcji definicje oznaczają odpowiednio:

1. **Administrator** - Ghelamco Poland spółka z ograniczoną odpowiedzialnością z siedzibą w Warszawie, adres: pl. Europejski 1, 00-844 Warszawa, wpisaną pod nr KRS 0000767269 do rejestru przedsiębiorców KRS, prowadzonego przez Sąd Rejonowy dla m. st. Warszawy w Warszawie, XIII Wydział Gospodarczy KRS, REGON: 01139401600000,
2. **ASI** - administrator Systemu informatycznego będący Pracownikiem odpowiedzialnym za funkcjonowanie Systemu informatycznego oraz stosowanie Środków technicznych i organizacyjnych w tym systemie,
3. **Dane / Dane Osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, tj. osoby, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne,
4. **Instrukcja** - niniejsza instrukcja określająca sposób zarządzania Systemami informatycznymi służącymi do Przetwarzania Danych Osobowych obowiązujących u Administratora,
5. **Osoba upoważniona** - Pracownik posiadający pisemne Upoważnienie do Przetwarzania Danych Osobowych wydane przez Administratora, umożliwiające Przetwarzanie Danych Osobowych w Systemie informatycznym w zakresie w nim wskazanym,
6. **Pracownik** - osoba fizyczna zatrudniona przez Administratora na podstawie umowy o pracę lub współpracująca z Administratorem na podstawie umowy zlecenia, umowy o dzieło lub innej umowy cywilnoprawnej,
7. **Przetwarzanie Danych Osobowych** - oznacza operację lub zestaw operacji wykonywanych na Danych Osobowych lub zestawach Danych Osobowych w sposób zautomatyzowany lub niezautomatyzowany, taki 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,

8. **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych u Administratora w celu Przetwarzania Danych Osobowych, w tym procedury awaryjne,
9. **Środki techniczne i organizacyjne** - środki bezpieczeństwa Przetwarzania Danych Osobowych określone w Ustawie oraz w RODO,
10. **Upoważnienie do Przetwarzania Danych Osobowych** - dokument uprawniający wskazaną w nim osobę do Przetwarzania Danych Osobowych u Administratora,
11. **Ustawa** - Ustawa o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz.U.2018.1000 z dnia 2018.05.24 z późn. zm.), jak również Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz.U. Nr 133, poz. 883 z późn. zm.), w zakresie obowiązujących przepisów,
12. **Użytkownik Systemu informatycznego** - Osoba upoważniona do Przetwarzania Danych Osobowych w Systemie informatycznym (dalej także jako Użytkownik),

§2

ASI I JEGO ZASTĘPCY

1. ASI jest odpowiedzialny za zarządzanie Systemem informatycznym.
2. ASI jest odpowiedzialny w szczególności za:
   a) nadawanie i odwoływanie uprawnień Użytkownikom Systemu informatycznego, w tym uprawnień do korzystania z poszczególnych programów i aplikacji w Systemie informatycznym,
   b) stosowanie metod i środków uwierzytelniania Użytkowników Systemu informatycznego,
   c) tworzenie kopii zapasowych zbiorów Danych oraz programów i narzędzi programowych służących do ich przechowywania, a także przechowywanie kopii zapasowych,
   d) zabezpieczenie Systemu informatycznego przed wirusami i szkodliwym oprogramowaniem, a także przed utratą Danych z powodu awarii zasilania lub zakłóceń sieci zasilającej,
   e) wykonywanie przeglądów i konserwacji Systemu informatycznego,
   f) sprawdzanie, czy Dane Osobowe przechowywane przez Użytkowników Systemu informatycznego są prawidłowo zabezpieczone.
3. ASI zobowiązany jest do wykonywania decyzji i poleceń zarządu Administratora, a także realizowania jego wytycznych.
4. Administrator powołuje dwóch zastępców ASI, którzy są odpowiedzialni odpowiednio za zarządzanie systemami informatycznymi Perseus i Primavera.
5. Zakres uprawnień oraz obowiązków ASI, stosuje się odpowiednio do zastępców ASI w odniesieniu do systemów informatycznych Perseus i Primavera.
6. Pracownicy mają stałą możliwość zadawania pytań szczegółowych w przypadku posiadania wątpliwości oraz uzyskania wiążącej odpowiedzi. Zapytania należy kierować do Administratora lub ASI, z którym można się skontaktować poprzez ITSupport@ghelamco.com.

§3

PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM ORAZ WSKAZANIE OSOBY ODPOWIEDZIALNEJ ZA TE CZYNNOŚCI

1. Przetwarzać Dane Osobowe w Systemie informatycznym może wyłącznie Pracownik, który posiada pisemne Upoważnienie do Przetwarzania Danych Osobowych.
2. Upoważnienie do Przetwarzania Danych Osobowych wydawane jest przez Administratora.
3. Oryginał Upoważnienia do Przetwarzania Danych Osobowych znajduje się u Administratora. Odpis Upoważnienia do Przetwarzania Danych Osobowych przekazywany jest Pracownikowi za pisemnym potwierdzeniem odbioru. Administrator otrzymuje odpis Upoważnienia do Przetwarzania Danych Osobowych wraz z pisemnym potwierdzeniem jego odbioru przez Pracownika. Odpis Upoważnienia do Przetwarzania Danych Osobowych przechowywany jest w dziale personalnym Administratora.
4. ASI upoważniony jest do przyznawania Użytkownikowi uprawnień do danego zbioru Danych Osobowych w węższym zakresie niż wskazanym w Upoważnieniu do Przetwarzania Danych Osobowych. Przyznanie przez ASI węższych uprawnień nie wymaga zmiany treści Upoważnienia do Przetwarzania Danych.
5. Każdej Osobie upoważnionej zakładane jest konto oraz przydzielany oddzielny identyfikator i hasło dostępu do Systemu informatycznego.
6. Za utworzenie konta oraz przydzielenie i wygenerowanie identyfikatora oraz pierwszego hasła dostępu do Systemu informatycznego odpowiada ASI.
7. Administrator prowadzi ewidencję Osób upoważnionych.
8. Hasło do Systemu informatycznego powinna znać jedynie osoba upoważniona.
9. Do zmiany identyfikatorów uprawniony jest ASI.
10. W przypadku cofnięcia Upoważnienia do Przetwarzania Danych Osobowych, a także w przypadku wygaśnięcia statusu Pracownika, identyfikator i hasło nic mogą być przypisane innej osobie.
11. Administrowanie i serwisowanie Systemu informatycznego oraz programów informatycznych służących do jego obsługi, wykonywane jest przez ASI.

§4

STOSOWANE METODY I ŚRODKI UWIERZYTELNIANIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM

1. Co do zasady uwierzytelnienie Osoby upoważnionej w Systemie informatycznym następuje po podaniu przez nią nazwy identyfikatora i hasła dostępu.
2. Hasła dostępu do Systemu informatycznego są przechowywane w Systemie Informatycznym w formie zaszyfrowanej, bez możliwości podglądu hasła przez inne Osoby upoważnione oraz ASI, Osoba upoważniona nie może udostępniać swojego identyfikatora ani hasła dostępu osobom trzecim. Osoba upoważniona nie może także zapisywać identyfikatora ani hasła w miejscu dostępnym dla osób nieuprawnionych.
3. Osoba upoważniona odpowiedzialna jest za wszystkie czynności wykonane przy użyciu identyfikatora, którym posługuje lub posługiwała się jako Użytkownik Systemu Informatycznego.

4. Identyfikator składa się co najmniej z 5 znaków, z wyłączeniem systemu Primavera, w którym identyfikator może składać się z 3 znaków. Identyfikator nie zawiera polskich liter.
5. Hasło składa się co najmniej z 8 znaków zawierających małe i wielkie litery oraz cyfry lub znaki specjalne. Hasło Użytkownika Systemu informatycznego nie może być takie samo jak identyfikator.
6. Hasło Użytkownika Systemu informatycznego nie może być zapisane w miejscu dostępnym dla osób nieuprawnionych.
7. Hasło dostępu przydzielone Użytkownikowi Systemu informatycznego musi być zmienione przez niego po pierwszym zalogowaniu się do Systemu informatycznego. Hasło dostępu powinno być zmieniane przez Użytkownika Systemu informatycznego nie rzadziej niż raz na 42 dni.
8. Zabezpieczenia przed nieautoryzowanym dostępem do przetwarzanych Danych osobowych poprzez Internet będzie odbywać się poprzez stosowanie systemu zapór ogniowych z sondami IPS.
9. W przypadku podejrzenia naruszenia poufności hasła, Użytkownik Systemu informatycznego zobowiązany jest niezwłocznie zmienić hasło i powiadomić o tym fakcie ASI.

§5

PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONE DLA UŻYTKOWNIKÓW SYSTEMU INFORMATYCZNEGO

1. Przed przystąpieniem do pracy w Systemie informatycznym, Użytkownik Systemu informatycznego zobowiązany jest sprawdzić komputer i stanowisko pracy ze zwróceniem uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony Danych Osobowych. W przypadku podejrzenia naruszenia bezpieczeństwa ochrony Danych Osobowych, Użytkownik Systemu informatycznego niezwłocznie powiadamia Administratora lub ASI. W przypadku braku możliwości zawiadomienia Administratora, należy zawiadomić bezpośredniego przełożonego.
2. Użytkownik Systemu informatycznego rozpoczyna pracę w Systemie informatycznym od następujących czynności:
   a) włączenia komputera,
   b) uwierzytelnienia się („zalogowania" w systemie) za pomocą identyfikatora i hasła.
3. Rozpoczęcie pracy w Systemie informatycznym może rozpocząć się od podania czterocyfrowego kodu PIN w celu odszyfrowania dysku twardego, o ile wykorzystywana metoda szyfrowania tego wymaga.
4. Niedopuszczalne jest uwierzytelnianie się na hasło i identyfikator innego Użytkownika Systemu informatycznego lub praca w Systemie informatycznym na koncie innego Użytkownika Systemu informatycznego.
5. Niedozwolone jest pozostawienie włączonego komputera w stanie oczekującym na podanie hasła.
6. W przypadku dłuższego opuszczenia stanowiska pracy Użytkownik Systemu informatycznego zobowiązany jest „wylogować się" lub zaktywizować wygaszacz ekranu z opcją ponownego „logowania" się do Systemu Informatycznego. Automatyczne wygaszenie ekranu będzie następowało po 5 minutach nieaktywności komputera. Odblokowanie sesji następuje po podaniu hasła przez Użytkownika Systemu informatycznego.
7. Po zakończeniu pracy w Systemie informatycznym, Użytkownik Systemu informatycznego powinien „wylogować się" oraz wyłączyć komputer. Użytkownik Systemu informatycznego powinien także

zabezpieczyć swoje stanowisko pracy, w szczególności nośniki danych, dokumenty i wydruki zawierające Dane Osobowe, przed dostępem osób nieupoważnionych.

§6

PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH OSOBOWYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

1. Kopie zapasowe zbiorów Danych Osobowych sporządzane są przez Użytkownika Systemu informatycznego każdego dnia po zakończeniem pracy w Systemie informatycznym. Tworzenie kopii zapasowych odbywa się przy pomocy oprogramowania Veeam oraz Nakivo.
2. Tworzenie kopii zapasowych odbywa się według następującego harmonogramu:
   a) kopie aktualnych zbiorów danych oraz istotnych elementów systemu operacyjnego serwera głównego są wykonywane codziennie; kopie są wykonywane poprzez kopię migawkową serwera w procesie Disk-To-Disk na macierz dyskową.
   b) Uzyskane kopie zapasowe są następnie replikowane na macierz dyskową zlokalizowaną w zapasowej serwerowni poza budynkiem.
3. Niezależnie od powyższego procesu tworzenia kopii zapasowych, w trakcie godzin pracy użytkowników tworzone są kopie migawkowe z poziomu systemu operacyjnego serwera, przechowywane do 12 godzin.
4. Macierz dyskowa zawierająca kopie zapasowe znajduje się w serwerowni, do której dostęp mają jedynie wyznaczone osoby w firmie. ASI okresowo sprawdza możliwość odtworzenia danych z kopii zapasowych.
5. Kopie zapasowe są przechowywane według następującego scenariusza:
   a) Kopie główne dzienne przez 10 dni.
   b) Kopie główne tygodniowe przez 4 tygodnie
   c) Kopie główne miesięczne przez 12 miesięcy
   d) Kopie główne roczne przez 3 lata.
   e) Repliki kopii głównych rocznych przez okres posiadania przez Administratora podstawy prawnej do przechowywanych Danych.
6. Pliki zawierające Dane Osobowe u Administratora, co do zasady znajdują się na dysku centralnym znajdującym się w siedzibie Administratora Danych Osobowych. Pliki wskazane w zdaniu poprzedzającym mogą być kopiowane na określony czas przez Użytkowników Systemu informatycznego na dyski lokalne. Po ustaniu ich przydatności, Użytkownik Systemu informatycznego jest zobowiązany niezwłocznie usunąć pliki zawierające Dane Osobowe.
7. Ewentualne wydruki zawierające Dane Osobowe, przechowywane są w miejscu uniemożliwiającym dostęp do nich osobom nieupoważnionym.

ur

§7

SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE ORAZ KOPII ZAPASOWYCH

1. Nośniki Danych Osobowych zarówno w postaci elektronicznej, jak i papierowej powinny być zabezpieczone przed dostępem osób nieuprawnionych, nieautoryzowaną modyfikacją oraz zniszczeniem, poprzez szyfrowanie.
2. Dane Osobowe mogą być zapisywane na nośnikach przenośnych tylko w przypadku tworzenia kopii zapasowych lub gdy istnieje konieczność przeniesienia tych Danych w postaci elektronicznej. Przed zapisem wymagane jest zaszyfrowanie nośnika.
3. Osoba upoważniona sporządzająca wydruk zawierający Dane Osobowe ma obowiązek na bieżąco sprawdzać przydatność wydruku, a w przypadku braku jego przydatności - niezwłocznie zniszczyć go w niszczarce.
4. Elektroniczne nośniki zawierające Dane Osobowe oraz wydruki powinny być przechowywane w zamkniętych szafach wewnątrz pomieszczeń, w których przetwarzane są Dane Osobowe i nie powinny być bez uzasadnionej przyczyny wynoszone poza te pomieszczenia.
5. Po zakończeniu przydatności nośnika zawierającego Dane Osobowe należy przeprowadzić nieodwracalne usunięcie Danych Osobowych z tego nośnika.
6. W przypadku uszkodzenia lub zużycia nośnika informacji zawierającego Dane Osobowe należy go fizycznie zniszczyć tak, aby nie było możliwe odczytanie Danych Osobowych.
7. Dokumenty w formie elektronicznej zawierające zbiory Danych Osobowych powinny być chronione hasłem. Inne pliki, które nic posiadają wbudowanych mechanizmów do założenia hasła, będą zamieszczane w archiwum .zip zabezpieczonym hasłem.
8. Ochrona Danych Osobowych, zawartych w plikach, będzie zapewniana również poprzez nadanie odpowiednich uprawnień Owner/Editor/Reader w platformie SharePoint.

§8

SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO

1. Na każdym stanowisku komputerowym powinno być zainstalowane oprogramowanie zabezpieczające, antywirusowe i szyfrujące (np. Symantec Endpoint Protection, Kaspersky Endpoint Security, HP Drive Lock, MS BitLocker).
2. Każdy e-mail wpływający na konta pocztowe Użytkownika Systemu informatycznego musi być sprawdzony pod kątem występowania wirusów przez oprogramowanie antywirusowe.
3. Definicje wzorców wirusów aktualizowane są nie rzadziej niż 1 raz dziennie.
4. Użytkownikom Systemu informatycznego zabrania się:
   a) używania nośników niewiadomego pochodzenia,
   b) instalowania oprogramowania bez zgody ASI.

5. ASI przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach - minimum raz w tygodniu.
6. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania.
7. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe, na którym wirusa wykryto oraz wszystkie posiadane przez użytkownika nośniki.

§9

SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED UTRATĄ DANYCH OSOBOWYCH SPOWODOWANĄ AWARIĄ ZASILANIA LUB ZAKŁÓCENIA W SIECI ZASILAJĄCEJ

1. Serwery informatyczne, na których gromadzone są Dane Osobowe, wyposażone są w redundantne zasilanie z redundantnym podtrzymaniem bateryjnym (zasilanie dodatkowe).
2. Serwery informatyczne mogą funkcjonować na zasilaniu dodatkowym przez 30 minut. Po upływie tego czasu inicjowana jest procedura bezpiecznego wyłączenia Systemów Informatycznych.
3. O każdej awarii Systemu Informatycznego, ASI zobowiązany jest niezwłocznie poinformować Administratora, wskazując jednocześnie przyczynę awarii zasilania lub zakłócenia w sieci zasilającej.

§10

ZASADY I SPOSÓB ODNOTOWYWANIA INFORMACJI O UDOSTĘPNIENIU DANYCH OSOBOWYCH

1. Administrator prowadzi rejestr czynności przetwarzania Danych Osobowych, rejestr żądań osób, których Dane Osobowe są przetwarzane, jak również rejestr naruszeń.
2. System informatyczny powinien zapewnić możliwość sporządzenia skanu lub wydruku, w sposób pozwalający na odczytanie informacji, o których mowa w ust. 1 powyżej.

§11

PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMU INFORMATYCZNEGO ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Przeglądy i konserwacja urządzeń wchodzących w skład Systemu informatycznego powinny być wykonywane w terminach określonych przez producenta sprzętu.
2. Nieprawidłowości ujawnione w trakcie działań wskazanych w ust. 1 powyżej powinny być niezwłoczne usunięte, a informacja o ujawnionych nieprawidłowościach powinna być niezwłocznie przekazana do Administratora wraz ze wskazaniem przyczyny nieprawidłowości oraz sposobu jej usunięcia.
3. ASI prowadzi dokumentację przeglądów i konserwacji Systemu informatycznego.

§12

ZASADY KORZYSTANIA Z URZĄDZEŃ MOBLINYCH

1. Przetwarzanie Danych Osobowych na urządzeniach mobilnych (laptopach, tabletach, telefonach itp.) używanych przez Pracowników odbywa się na zasadach określonych w Polityce oraz w Instrukcji, z uwzględnieniem niniejszego paragrafu.
2. Przetwarzanie Danych Osobowych na urządzeniach mobilnych jest możliwe po powiadomieniu o tym Administratora.
3. Pracownik korzystający z urządzenia mobilnego zobowiązany jest do:
   a) przenoszenia urządzenia mobilnego w sposób minimalizujący ryzyko kradzieży, zagubienia lub zniszczenia,
   b) uniemożliwienia osobom trzecim dostępu do urządzenia mobilnego,
   c) zabezpieczenia urządzenia mobilnego hasłem i utrzymanie konfiguracji oprogramowania systemowego w stanie wymuszającym korzystanie z tego hasła.

§13

PROCEDURA I ŚRODKI OCHRONY SYSTEMU INFORMATYCZNEGO

Szczegółowy opis procedur oraz środków, stosowanych przez Administratora w celu zapewnienia bezpieczeństwa Systemów informatycznych, stanowi **Załącznik nr 1** do Instrukcji.

§14

OCHRONA DANYCH OSOBOWYCH

1. U Administratora istnieje zakaz wykonywania kopii lub skanów dowodów osobistych (paszportów/praw jazdy itp.) kontrahentów, klientów lub podwykonawców Administratora.
2. U Administratora istnieje zakaz dołączania kopii dowodów osobistych wskazanych w ust.1 do żadnych umów lub innych dokumentów.
3. U Administratora istnieje zakaz wysyłania próśb do kontrahentów o przesyłanie skanów dowodów osobistych. Dane Osobowe z dowodów osobistych należy pozyskiwać przy okazji spotkania przy podpisaniu umowy - lub za pomocą prośby o przesłanie odpowiednich Danych Osobowych – mailem.
4. Pracownicy ograniczają zbieranie Danych Osobowych tylko do niezbędnych Danych Osobowych, tzn. tylko takich, jakie są potrzebne, np. niezbędne do wypełnienia umowy wg wzoru – zakaz zbierania Danych Osobowych na zapas albo „na wszelki wypadek".
5. Pracownicy mają zakaz przekazywania Danych Osobowych klientów Administratora będących osobami fizycznymi podwykonawcom:
   a) bez wyraźnej pisemnej (w tym mailowej) zgody klienta. Jeśli podwykonawca Administratora chce się skontaktować z klientem Administratora, ponieważ np. podwykonawca Administratora chce klientowi Administratora wysłać ofertę i Administrator nie widzi w tym przeszkód, to należy napisać do naszego klienta z pytaniem, czy Administrator może przekazać jego imię, nazwisko, nr mieszkania, telefon albo adres e - mail do firmy „X". Bez wyraźnej zgody wyrażonej przez klienta Administratora nie wolno przekazać Danych Osobowych klienta Administratora żadnemu podwykonawcy.

6. Pracownicy mają zakaz przekazywania Danych Osobowych klientów Administratora, będących osobami fizycznymi, innym klientom Administratora bez wyraźnej pisemnej (w tym mailowej) zgody klienta. Bez odpowiedniej zgody nie wolno przekazać Danych Osobowych klientów żadnym osobom.

7. Pracownicy mają obowiązek szyfrowania/zabezpieczania hasłem wszystkich plików zawierających zestawienia Danych Osobowych, które zapisywane są na pendrivach. Instrukcja szyfrowania/zabezpieczania hasłem plików zapisywanych na pendrivach zostanie przedstawiona na prośbę.

8. Pracownicy mają obowiązek zabezpieczania hasłem wszystkich plików office zachowywanych na komputerach zawierających listy osób np. lista do rozesłania prezentów, listy klientów, listy kontaktowe. Inne pliki, które nie posiadają wbudowanych mechanizmów do nałożenia hasła, muszą zostać umieszczone w archiwum .zip, a na to archiwum należy nałożyć hasło. W przypadku wysłania takiej listy mailem dalej, to hasło dostępu przekazujemy innym kanałem najlepiej w trakcie bezpośredniej rozmowy lub SMS. W przypadku otrzymywania list od kontrahentów (np. lista pracowników wykonawcy wchodzących na budowę, przekazywana w wersji elektronicznej), żądamy od kontrahentów, aby dokument przesyłany w wersji elektronicznej zawierający takie listy był zabezpieczony hasłem.

9. W przypadku konieczności udostępnienia umowy z klientem będącym osobą fizyczną dalszym podwykonawcom, np. w celu wykończenia mieszkania, zgodnie z jej treścią, Pracownik musi zamazać Dane Osobowe tego klienta (oraz zawsze cenę) - tak, aby nie były czytelne.

10. Polityka czystego biurka: żadna umowa z osobą fizyczną nie może być pozostawiona na biurku na czas po zakończeniu pracy w danym dniu – powinna być schowana do szafki zamkniętej na klucz. Powyższe dotyczy także takich dokumentów jak faktury lub inne dokumenty, które zawierają Dane Osobowe klientów - osób fizycznych. Czystość biurek będzie systematycznie kontrolowana.

11. Pracownicy mają obowiązek wygaszania ekranu - musi być ustawiony automatycznie na wygaszenie nie później niż po 5 minutach braku aktywności.

12. Pracownicy mają obowiązek ustawienia haseł dostępu do telefonów komórkowych używanych dla celów służbowych.

13. Pracownicy mają zakaz wysyłania maili do dużej liczby odbiorców spoza biura, umieszczając ich adresy mailowe w polu CC (DW). Jeśli wiadomość e-mail ma więcej niż 10 odbiorców to prosimy umieszczać ich adresy mailowe w polu BCC (UDW), chyba że wszyscy odbiorcy pracują nad daną transakcją/tematem/umową i jest to niezbędne do należytego procedowania danego tematu. Do klientów działu RESI oraz osób, które podają swoje Dane Osobowe dla potrzeb organizowanych różnych konkursów – w żadnym wypadku (niezależnie od ilości adresatów) przy korespondencji zbiorczej Pracownikom nie wolno umieszczać adresów mailowych w polu CC (DW), tylko zawsze w polu BCC (UDW).

14. W przypadku mailingu typu życzenia świąteczne lub zaproszenie na event koniecznie adresy mailowe odbiorców należy umieścić w polu BCC (UDW) - nigdy w CC (DW).

15. W przypadku pierwszego kontaktu z klientem będącym osobą fizyczną, Pracownik przekazuje mu klauzulę informacyjną - klient powinien potwierdzić, że się zapoznał poprzez złożenie podpisu lub potwierdzenie elektroniczne; Powyższe ma przede wszystkich zastosowanie dla działu RESI, działu Komercji w zakresie najmu na rzecz osób fizycznych nie prowadzących działalności gospodarczej - najczęściej najem miejsc parkingowych, działu marketingu przy organizacji konkursów. Osoby zainteresowane otrzymaniem klauzuli informacyjnej prosimy o kontakt z działem prawnym.

16. Pracownicy zamieszczają w stopce klauzulę informacyjną przynajmniej przy pierwszym mailach z daną osobą. Wzór stopki można znaleźć:

    a) dla wszystkich działów poza RESI [DMS -> Document tamplates -> RODO -> stopki mailowe -> 2018.06.07 stopka mailowa_wszystkie działy poza RESI;

    b) wyłącznie dla działu RESI [DMS -> Document tamplates -> RODO -> stopki mailowe -> 2018.06.07 stopka mailowa_wyłącznie dział RESI.

17. W przypadku zgubienia/utraty nośnika zawierającego Dane Osobowe np. pendrive, laptopa, smartfonu, Pracownik natychmiast zgłasza tę informacje pod adres RODO@ghelamco.pl. Jeżeli niechcący wysłano maila zawierającego listy Danych/dane wrażliwe do osoby nieuprawnionej, albo podejrzewa się, że ktoś uzyskał nieuprawniony dostęp do systemu albo Danych Osobowych – Pracownik natychmiast zgłasza tę informację pod adres RODO@ghelamco.pl.

18. Drukując/skanując/kopiując dokument zawierający zestawienie Danych Osobowych np. lista kontaktowa, lista pracowników wchodzących na budowę, lista gości zaproszonych na eventy, lista osób uczestniczących w szkoleniu, konkursie, załączników do faktury zawierających listę osób biorących udziału jakimś wydarzeniu, korzystających z określonych benefitów – należy zachować szczególną ostrożność tak, aby nikt inny nie miał możliwości zapoznania się z treścią tych dokumentów.

19. Jeżeli spodziewane jest otrzymanie faksu – Pracownik ma obowiązek pilnować w copy roomie jego natychmiastowego odbioru, aby faks ten trafił tylko do nas i nikt inny nie zapoznał się z jego treścią.

20. Wszystkie dokumenty zawierające Dane Osobowe, w celu ich zniszczenia – Pracownik ma obowiązek wrzucać do zaplombowanych kontenerów albo zniszczyć je w niszczarce – nie wolno wrzucać do kosza.

21. W razie wątpliwości Pracownicy mogą kierować wszelkie pytania do działu prawnego - najchętniej mailowo na adres: rodo@ghelamco.pl.

§ 15

ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ I PLATFORM WYMIANY PLIKÓW

1. W przypadku korzystania przez Pracowników z platform wymiany plików, w szczególności takich jak Box, DropBox, Google Drive, użytkownicy zobowiązani są do szczególnej ostrożności. Administrator Danych przekaże Pracownikom informacje w zakresie zasad korzystania z tego rodzaju platform w przypadku ich wykorzystywania przez Pracowników.

2. W przypadku przesyłania Danych Osobowych mailem zawarli w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.

3. Zabrania się otwierania załączników (.zip, .xlsm, .pdf, .exe) w mailach od nieznanych nadawców. Nie wolno także otwierać hiperlinków.

4. Należy zgłaszać Administratorowi Danych przypadki podejrzanych e-maili.

5. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości".

6. Pracownicy powinni okresowo kasować nieaktualne maile.

7. Konta pocztowe firmowe są odseparowane od poczty prywatnej.
8. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.
9. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe Pracowników lub innych osób.
10. Pracownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
11. Zabrania się Pracownikom konfigurowania swoich kont pocztowych do automatycznego przekierowywania wiadomości na adres zewnętrzny.
12. Korzystanie z maila dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Pracowników pracy/usług oraz na prawidłowe i rzetelne wykonywanie przez nich obowiązków służbowych.
13. Przy korzystaniu z maila, Pracownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
14. Pracownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.
15. Pracownicy bez zgody Administratora Danych nie mają prawa wysyłać wiadomości zawierających Dane Osobowe dotyczące Pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

§ 16

ZASADY POSTĘPOWANIA PRZY NARUSZENIU OCHRONY DANYCH OSOBOWYCH

1. W wypadku wystąpienia zagrożenia naruszenia bezpieczeństwa ochrony Danych poprzez utratę kontroli bądź chwilową utratę kontroli nad sprzętem komputerowym, na którym Dane te są zgromadzone, Pracownicy zobowiązani są niezwłocznie zawiadomić zarząd Administratora lub ASI.
2. Utrata kontroli może w szczególności oznaczać nieautoryzowany dostęp do sprzętu komputerowego przez osobę nieupoważnioną, długotrwałe zgubienie sprzętu lub jego kradzież.
3. Chwilowa utrata kontroli może w szczególności oznaczać czasowe pozostawienie sprzętu komputerowego w miejscu gdzie osoby nieupoważnione mogły mieć do niego dostęp (np. kawiarnia, czytelnia, metro lub inne miejsce ogólnie dostępne).
4. W wypadku wystąpienia mechanicznego zagrożenia naruszenia bezpieczeństwa ochrony Danych, poprzez mechaniczne uszkodzenie sprzętu komputerowego (np. zalanie sprzętu cieczą, spięcie elektryczne, mechaniczne uszkodzenie sprzętu), Pracownicy zobowiązani są niezwłocznie zawiadomić zarząd Administratora lub ASI.
5. Po dokonaniu zgłoszenia przez Pracowników, ASI wraz z zarządem Administratora sprawdza czy w okresie utraty bądź chwilowej utraty kontroli nad sprzętem komputerowym, bezpieczeństwo Danych Osobowych zgromadzonych na sprzęcie nie zostało naruszone, a jeśli tak, to w jaki sposób oraz w jakim stopniu. W przypadku mechanicznego uszkodzenia sprzętu, przeprowadza się sprawdzenie, czy takie uszkodzenie nie wpłynęło na integralność bądź nie doprowadziło do usunięcia Danych na takim sprzęcie.
6. Po dokonaniu sprawdzenia zgłoszenia, ASI wraz z zarządem Administratora podejmują stosowne

ш

decyzje w zakresie powiadamiania lub nie Prezesa Urzędu Ochrony Danych Osobowych lub/ i osób których Dane dotyczą.

§ 17

AKTUALIZACJA INSTRUKCJI

1. Instrukcja podlega przeglądowi oraz ewentualnej aktualizacji każdorazowo w przypadku:
   a) zmiany przepisów dotyczących ochrony Danych Osobowych,
   b) znaczących zmian w zakresie zapewnienia bezpieczeństwa ochrony Danych Osobowych Przetwarzanych u Administratora.
2. Przeglądu i aktualizacji Instrukcji dokonuje zarząd Administratora.

§18

POSTANOWIENIA KOŃCOWE

1. W zakresie nieuregulowanym Instrukcją zastosowanie znajdą przepisy Ustawy oraz RODO oraz postanowienia Polityki.
2. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z wewnętrznych regulacji Polityki oraz dokumentów powiązanych, mogą zostać potraktowane przez Administratora, w zależności od ich wagi i rozmiaru skutków, jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.
3. Instrukcja została przyjęta przez Administratora w dniu 12 lipca 2021 roku.

Jeroen van der Toolen

Członek Zarządu

ZAŁĄCZNIK NR 1

DO INSTRUKCJI OKREŚLAJĄCEJ SPOSÓB ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI SŁUŻĄCYMI DO PRZETWARZANIA DANYCH OSOBOWYCH OBOWIĄZUJĄCYCH
W GHELAMCO POLAND SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

Polityka bezpieczeństwa Systemów informatycznych

Wprowadzenie

W celu zapewnienia bezpieczeństwa, spójności i integralności Systemów informatycznych oraz ochrony Danych przechowywanych i przetwarzanych w tych Systemach, spółka Ghelamco Poland spółka z ograniczoną odpowiedzialnością wdrożyła niżej wymienione polityki oraz procedury korzystania z tych Systemów, jak również dedykowane rozwiązania sprzętowe i programowe, chroniące te Systemy przed naruszeniami tychże polityk i procedur. Systemy te są na bieżąco monitorowane, a raporty o nieprawidłowościach i naruszeniach przekazywane do działu IT.

Ochrona stanowiska pracy

- Kontrola dostępu do powierzchni biura oparta o karty zbliżeniowe.
- Separacja strefy gości i pracowniczej na powierzchni biurowej z wykorzystaniem kontroli dostępu.
- Monitoring wizyjny wejść i wyjść z powierzchni biura oraz przejść pomiędzy strefami gości i pracowniczej.

Ochrona stacji roboczych i komputerów przenośnych

- BIOS zabezpieczony hasłem IT, z zablokowanymi możliwościami uruchomienia komputera z nośników przenośnych lub sieci.
- Zaszyfrowany dysk twardy (BitLocker, DriveLock with SED).
- Logowanie do komputera w oparciu o indywidualne konta w domenie Active Directory.
- Hasła z wymogiem złożoności, historii wykorzystania oraz podlegające regularnym zmianom.
- Zakaz przekazywania haseł innym osobom, w tym IT.
- Ochrona aktualizowanym na bieżąco oprogramowaniem antywirusowym (Kaspersky) z aktywnym modułem zapory ogniowej oraz wykrywaniem anomalii w zachowaniu aplikacji.
- Zaplanowane cotygodniowe pełne skanowanie oprogramowaniem antywirusowym.
- Raportowanie o stanie ochrony antywirusowej w tym o wykryciu zagrożenia, bądź braku aktualizacji.
- Brak uprawnień administracyjnych na kontach użytkowników.
- Automatyczna aktualizacja systemu operacyjnego i aplikacji poprzez wewnętrzny serwer dystrybucji.
- Automatyczne blokowanie stanowiska pracy po 5 minutach bezczynności.
- Szyfrowanie nośników USB przed zapisem na nich danych.
- Wykorzystanie linek zabezpieczających (Kensington).

ш

Ochrona sieci

- Odseparowanie sieci dla gości i pracowniczej.
- Dostęp do sieci pracowniczej w oparciu o certyfikat.
- Odseparowanie sieci dostępowej, usług, zarządzania, monitoringu wizyjnego oraz telefonii stacjonarnej.
- Ruch pomiędzy sieciami ograniczony politykami dostępowymi na przełącznikach i zaporze ogniowej (Cisco Catalyst, Cisco ASA-X).
- Ruch przychodzący ograniczony politykami dostępowymi na zaporze ogniowej, skanowany i filtrowany sondami IPS (Cisco ASA-X).
- Ruch wychodzący skanowany pod kątem reputacji i klasyfikacji treści serwera docelowego (Cisco Firepower).
- Ruch do serwerów dostępnych z zewnątrz szyfrowany certyfikatem komercyjnym.
- Dostęp z zewnątrz dla wybranych Pracowników poprzez połączenie VPN (Cisco ASA-X).
- Ruch pomiędzy oddziałami z wykorzystaniem dedykowanych łączy światłowodowych (Netia Ethernet, MPLS), ograniczony politykami bezpieczeństwa na zaporach ogniowych (Cisco ASA-X, Zyxell USG, Unify USG).
- Redundantne łącza internetowe od niezależnych operatorów (Netia, ITSA).

Ochrona serwerowni i serwerów

- Kontrola dostępu w oparciu o karty zbliżeniowe tylko dla Pracowników IT oraz karty z bezpiecznej koperty.
- Monitoring wizyjny wnętrza serwerowni z sygnalizacją wykrycia ruchu.
- Czujka pożarowa z dedykowanym systemem gaszenia gazem.
- Redundantny system chłodzenia z sygnalizacją wzrostu temperatury.
- Serwery z redundantnymi zasilaczami (HP), korzystające z redundantnego systemu zasilania awaryjnego (APC).
- Maszyny wirtualne (VMWare) działające w oparciu o klaster dwóch serwerów, z możliwością migracji na trzeci serwer w serwerowni poza budynkiem.
- System kopii zapasowych przechowywanych poza serwerownią oraz replikacji poza budynek.
- System kopii zapasowych umożliwiający uruchomienie maszyny wirtualnej bezpośrednio z repozytorium kopii zapasowych.
- Polityka archiwizacji kopii zapasowych tygodniowych, miesięcznych i rocznych.

Ochrona wydruków

- Wydruki na drukarkach nabiurkowych w zasięgu wzroku użytkownika.
- Wydruki na drukarkach wielkoformatowych w dedykowanych pomieszczeniach, z wykorzystaniem systemu zwalniania wydruku (PaperCut).
- Polityka szyfrowania dysków twardych drukarek wielkoformatowych i bezpiecznego usuwania z pamięci zadań wykonanych.

Ochrona urządzeń mobilnych

- Polityka wymuszająca ochronę ekranu kodem lub odciskiem palca oraz blokująca ekran po 2 minutach bezczynności (Exchange ActiveSync).
- Szyfrowanie pamięci urządzenia.
- Ochrona oprogramowaniem antywirusowym urządzeń Android (Kaspersky).
- Weryfikacja reputacji stron www na urządzeniach iOS (SafeBrowser).
- Możliwość zdalnego zablokowania i wymazania danych z urządzenia.
- Możliwość lokalizacji ostatniego położenia GPS urządzenia.

Monitoring i raportowanie

- Logi urządzeń sieciowych zbierane w centralnym systemie archiwizacji i raportowania (Observium).
- Sygnalizacja poprzez e-mail i SMS naruszenia polityk bezpieczeństwa oprogramowania antywirusowego.
- Logowanie aktywności użytkownika i procesów działających na komputerach (WorkTime).

Polityki i procedury IT

- Rozszerzenie gwarancji na komputery o usługę on-site na 3/4/5 lat.
- Utrzymanie ważnego kontraktu serwisowego 24/7 na serwery i macierz dyskową.
- Utrzymanie ważnego kontraktu serwisowego na sprzęt drukujący.
- Utrzymanie ważnych subskrypcji dla wykorzystywanego oprogramowania z dostępem do aktualizacji i łat bezpieczeństwa (Microsoft, VMWare, PaperCut, WorkTime, Autodesk).
- Utrzymanie ważnych licencji na oprogramowanie ochronne (Kaspersky, Cisco FirePower).
- Szkolenia Pracowników z zakresu wykrywania i zachowań wobec zagrożeń pochodzących z poczty elektronicznej, stron internetowych i aplikacji mobilnych.
- Rozsyłanie alertów o bieżących zagrożeniach w sieci.

m

Procedura weryfikacji podmiotu przetwarzającego dane osobowe

Definicje:
Administrator danych - Ghelamco Poland sp. z o.o. z siedzibą w Warszawie, KRS: 0000767269;
IOD - Inspektor Ochrony Danych;
Procesor - [...];
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 (Ogólne Rozporządzenie o Ochronie Danych).

Nazwa oraz dane kontaktowe administratora danych	
Nazwa	Ghelamco Poland sp. z o.o.
Numer KRS, NIP, REGON	KRS: 0000767269 NIP: 5213637451 REGON: 146318915
Adres	pl. Europejski 1, 00-844 Warszawa
E-mail	rodo@ghelamco.pl
Telefon	22 455 16 00

Nazwa/ imię i nazwisko oraz dane kontaktowe podmiotu przetwarzającego dane osobowe	
Nazwa/ imię i nazwisko	[...]
Numer KRS, NIP, REGON	[...]
Adres	[...]
E-mail	[...]
Telefon	[...]

imię i nazwisko osoby udzielającej odpowiedzi na poniższe pytania	

Oświadczenie	konieczne wskazanie jednej z poniższych odpowiedzi: - tak - nie	własnoręczny podpis	data
W imieniu Procesora oświadczam, iż wszystkie podane poniżej informacje są zgodne z aktualnym stanem prawnym i faktycznym. W przypadku zmiany któregokolwiek z poniższych elementów, zobowiązuję się niezwłocznie (nie później niż w terminie 7 dni od wystąpienia zdarzenia) powiadomić o tym Administratora danych.			

WERYFIKACJA PODMIOTU PRZETWARZAJĄCEGO DANE OSOBOWE			
Lp.	**Pytanie**	**Odpowiedź**	**Uwagi**
Pytania dotyczące zagadnień organizacyjnych			
1.	Czy Procesor wyznaczył IOD? (w przypadku braku wyznaczenia IOD, należy wskazać dane innej osoby do kontaktu odpowiedzialnej za kwestie związane z ochroną danych osobowych).		Konieczne wskazanie jednej z poniższych odpowiedzi: - tak - nie - imię, nazwisko, adres, e-mail, nr telefonu osoby kontaktowej
2.	Czy pracownicy i kontrahenci Procesora zostali pouczeni o swojej odpowiedzialności za bezpieczeństwo informacji/ochronę danych osobowych i potwierdzili to pisemnymi oświadczeniami?		Konieczne wskazanie jednej z poniższych odpowiedzi: - tak - nie
3.	Czy Procesor wprowadził środki techniczne i organizacyjne, które będą: a) spełniały wymogi RODO oraz innych aktów regulujących przetwarzanie danych osobowych; b) chroniły prawa osób, których dane dotyczą?		Konieczne wskazanie jednej z poniższych odpowiedzi: - tak - nie
4.	Czy Procesor korzysta z dalszych procesorów (podprocesorów) w procesie przetwarzania danych osobowych na zlecenie administratora danych osobowych? a) w przypadku, gdy Procesor korzysta z dalszych procesorów (podprocesorzy), czy mają oni swoją siedzibę w ramach Europejskiego Obszaru Gospodarczego? b) czy podprocesorzy stosują środki techniczne i organizacyjne spełniające wymogi RODO?		Konieczne wskazanie jednej z poniższych odpowiedzi: - tak - nie
5.	Czy dane są przekazywane poza Europejski Obszar Gospodarczy? (w przypadku, gdy dochodzi do transferu danych poza Europejski Obszar Gospodarczy, na jakiej podstawie to następuje).		Konieczne wskazanie jednej z poniższych odpowiedzi: - tak - nie

6.	Czy Procesor nadał upoważnienia do przetwarzania powierzonych danych osobowych i zobowiązał do zachowania tajemnicy danych osobowyc?		Konieczne wskazanie jednej z poniższych odpowiedzi: - tak - nie
	Pytania dotyczące zagadnień proceduralnych		
7.	Czy Procesor prowadzi rejestr czynności dla powierzonych operacji przetwarzania danych osobowych?		Konieczne wskazanie jednej z poniższych odpowiedzi: - tak - nie
8.	Czy Procesor wdrożył procedury dotyczące zarządzania incydentami bezpieczeństwa?		Konieczne wskazanie jednej z poniższych odpowiedzi: - tak - nie
9.	Czy Procesor wdrożył zasady /procedurę /instrukcję powiadamiania podmiotu danych o naruszeniach danych osobowych?		Konieczne wskazanie jednej z poniższych odpowiedzi: - tak - nie
10.	Czy Procesor wdrożył mechanizmy usuwania danych po zakończeniu ich przetwarzania?		Konieczne wskazanie jednej z poniższych odpowiedzi: - tak - nie
	Pytania dotyczące zagadnień bezpieczeństwa		
11.	Czy Procesor wprowadził środki zapewniające, że systemy IT używane do przetwarzania danych osobowych są zgodne z RODO oraz innymi aktami regulującymi przetwarzanie danych osobowych?		Konieczne wskazanie jednej z poniższych odpowiedzi: - tak - nie
12.	Czy Procesor zapewnia adekwatną ochronę danych np. szyfrowanie danych, szyfrowanie połączeń zdalnych/sieciowych, itp.?		Konieczne wskazanie jednej z poniższych odpowiedzi: - tak - nie
13.	Czy Procesor wdrożył środki ochrony przed szkodliwym oprogramowaniem (malware) takim jak wirusy, robaki, konie trojańskie, itp.?		Konieczne wskazanie jednej z poniższych odpowiedzi: - tak - nie
14.	Czy Procesor wdrożył środki ochrony na wypadek awarii, takie jak plany awaryjne, środowiska zapasowe, kopie zapasowe, lub inne?		Konieczne wskazanie jednej z poniższych odpowiedzi: - tak - nie
15.	Czy Procesor przechodzi regularne audyty z zakresu bezpieczeństwa danych? (Jeśli tak, to z jaką częstotliwością i czy dostępne są raporty z audytu?)		Konieczne wskazanie jednej z poniższych odpowiedzi: - tak - nie
16.	Czy Procesor posiada aktualny certyfikat ISO 27001 lub inne równoważne certyfikaty?		Konieczne wskazanie jednej z poniższych odpowiedzi: - tak - nie
17.	Jakie sposoby zabezpieczenia pomieszczeń są wykorzystywane przez Procesora?		Przykładowe odpowiedzi: - drzwi zamykane na klucze; - drzwi z zamkami patentowymi; - drzwi wzmacniane; - drzwi antywłamaniowe

ZAŁĄCZNIK NR 3

LISTA SPÓŁEK Z GRUPY GHELAMCO

1	**Ghelamco Plac Vogla** spółka z ograniczoną odpowiedzialnością (dawniej: Ghelamco GP 1 Spółka z ograniczoną odpowiedzialnością Vogla S.K.A.)
2	GHELAMCO GP 11 Spółka z ograniczoną odpowiedzialnością **The HUB** S.K.A.
3	**Apollo Invest** Spółka z ograniczoną odpowiedzialnością
4	**Ghelamco Wronia** spółka z ograniczoną odpowiedzialnością (dawniej: Ghelamco GP 2 Spółka z ograniczoną odpowiedzialnością Sigma S.K.A.)
5	**Ghelamco The Bridge** spółka z ograniczoną odpowiedzialnością (dawniej: Ghelamco GP 9 Spółka z ograniczoną odpowiedzialnością Isola S.K.A.)
6	**Ghelamco Postępu** spółka z ograniczoną odpowiedzialnością (dawniej: Ghelamco GP 7 Spółka z ograniczoną odpowiedzialnością Postępu S.K.A.)
7	**Ghelamco Port Żerański** spółka z ograniczoną odpowiedzialnością (dawniej: Ghelamco GP 1 Spółka z ograniczoną odpowiedzialnością Port Żerański S.K.A.)
8	**SOBIESKI TOWERS** Spółka z ograniczoną odpowiedzialnością
9	**Ghelamco Plac Grzybowski** spółka z ograniczoną odpowiedzialnością (dawniej: Ghelamco GP 1 Spółka z ograniczoną odpowiedzialnością Unique S.K.A.)
10	**Ghelamco SBP** spółka z ograniczoną odpowiedzialnością (dawniej: Ghelamco GP 4 Spółka z ograniczoną odpowiedzialnością SBP S.K.A.)
11	**Ghealmco Craft** spółka z ograniczoną odpowiedzialnością (dawniej: Ghelamco GP 2 spółka z ograniczoną odpowiedzialnością Synergy S.K.A.)
12	Ollay spółka z ograniczoną odpowiedzialnością **Market** S.K.A.
13	**Erato** Spółka z ograniczoną odpowiedzialnością
14	**Ghelamco PIB** spółka z ograniczoną odpowiedzialnością (dawniej: Octon Spółka z ograniczoną odpowiedzialnością PIB S.K.A.)
15	Ghelamco GP 10 Spółka z ograniczoną odpowiedzialnością **Azira** S.K.A.
16	**P22 Łódź** spółka z ograniczoną odpowiedzialnością SP.K.
17	**Pianissima** Spółka z ograniczoną odpowiedzialnością
18	**Prima Bud** Spółka z ograniczoną odpowiedzialnością
19	**KEMBERTON** Spółka z ograniczoną odpowiedzialnością
20	**Estima** Spółka z ograniczoną odpowiedzialnością
21	**ABISAL** Spółka z ograniczoną odpowiedzialnością
22	**50 Dębów** Spółka z ograniczoną odpowiedzialnością
23	**X-Mas International** Spółka z ograniczoną odpowiedzialnością
24	**Ghelamco GP 3** Spółka z ograniczoną odpowiedzialnością
25	**Qanta** Spółka z ograniczoną odpowiedzialnością
26	**Ghelamco Towarowa** spółka z ograniczoną odpowiedzialnością (dawniej: Ghelamco GP 1 Spółka z ograniczoną odpowiedzialnością Azalia S.K.A.)
27	**Ghelamco Beta** spółka z ograniczoną odpowiedzialnością (dawniej: Ghelamco GP 1 Spółka z ograniczoną odpowiedzialnością Beta S.K.A.)
28	**Groen Konstancin II** spółka z ograniczoną odpowiedzialnością (daniej: Ghelamco GP 1 Spółka z ograniczoną odpowiedzialnością Tarima S.K.A.)
29	**Ghelamco PL 19** Spółka z ograniczoną odpowiedzialnością
30	Ghelamco PL 17 Spółka z ograniczoną odpowiedzialnością **Hotel** S.K.A.
31	**Signal OS sp. z o.o.** (dawniej: **MeetDistrict** Spółka z ograniczoną odpowiedzialnością)
32	**NCL Hotel** Spółka z ograniczoną odpowiedzialnością
33	**Ghelamco Zafina** spółka z ograniczoną odpowiedzialnością (dawniej: Ghelamco GP 2 spółka z ograniczoną odpowiedzialnością Zafina S.K.A.)
34	**Ghelamco Kreo** spółka z ograniczoną odpowiedzialnością (dawniej: Ghelamco GP 2 spółka z ograniczoną odpowiedzialnością Eurema S.K.A.)
35	**Ghelamco HQ** spółka z ograniczoną odpowiedzialnością (dawniej: Ghelamco GP 6 spółka z ograniczoną odpowiedzialnością HQ S.K.A.)
36	**Ghelamco Gdańska PI** Spółka z ograniczoną odpowiedzialnością
37	**Ghelamco Garden Station** Spółka z ograniczoną odpowiedzialnością
38	Ghelamco GP 10 Spółka z ograniczoną odpowiedzialnością **Arifa** S.K.A.
39	**Orrin** Spółka z ograniczoną odpowiedzialnością
40	**Ghelamco PL 18** Spółka z ograniczoną odpowiedzialnością
41	Ghelamco GP 2 spółka z ograniczoną odpowiedzialnością **M12** S.K.A.
42	Ghelamco GP 5 Spółka z ograniczoną odpowiedzialnością **CANNA** S.K.A.
43	Nowe Soho 1 spółka z ograniczoną odpowiedzialnością (dawniej: Ghelamco GP 10 Spółka z ograniczoną odpowiedzialnością NCŁ B1 S.K.A.)
44	Nowe Soho 2 spółka z ograniczoną odpowiedzialnością (dawniej: Ghelamco GP 10 Spółka z ograniczoną odpowiedzialnością NCŁ B2 S.K.A.)
45	Nowe Soho 3 spółka z ograniczoną odpowiedzialnością (dawniej: Ghelamco GP 10 Spółka z ograniczoną odpowiedzialnością NCŁ B3 S.K.A.)
46	Ghelamco GP 11 Spółka z ograniczoną odpowiedzialnością **EPONA** S.K.A.
47	**Octon** Spółka z ograniczoną odpowiedzialnością
48	**Ollay** Spółka z ograniczoną odpowiedzialnością
49	**Ghelamco GP 1** Spółka z ograniczoną odpowiedzialnością
50	**Ghelamco GP 2** Spółka z ograniczoną odpowiedzialnością
51	**Ghelamco GP 4** Spółka z ograniczoną odpowiedzialnością
52	**Ghelamco GP 5** Spółka z ograniczoną odpowiedzialnością
53	**Ghelamco GP 6** Spółka z ograniczoną odpowiedzialnością

54	**Ghelamco GP 7** Spółka z ograniczoną odpowiedzialnością
55	**Ghelamco GP 8** Spółka z ograniczoną odpowiedzialnością
56	**Ghelamco GP 9** Spółka z ograniczoną odpowiedzialnością
57	**Ghelamco GP 10** Spółka z ograniczoną odpowiedzialnością
58	**Ghelamco GP 11** Spółka z ograniczoną odpowiedzialnością
59	**Ghelamco PL 17** Spółka z ograniczoną odpowiedzialnością
60	**Ghelamco Invest** Spółka z ograniczoną odpowiedzialnością
61	**Innovation Bud Bis** Spółka z ograniczoną odpowiedzialnością
62	**Laboka Poland** Spółka z ograniczoną odpowiedzialnością
63	**Ilderim** Spółka z ograniczoną odpowiedzialnością
64	**P22 Łódź** Spółka z ograniczoną odpowiedzialnością
65	**Woronicza** Spółka z ograniczoną odpowiedzialnością
66	**Oaken** Spółka z ograniczoną odpowiedzialnością
67	**Orston** Spółka z ograniczoną odpowiedzialnością
68	**Oscroft** Spółka z ograniczoną odpowiedzialnością
69	**Skyfall Warsaw** spółka z ograniczoną odpowiedzialnością (dawniej: Luxus Invest Spółka z ograniczoną odpowiedzialnością)
70	**Wuza 2** Spółka z ograniczoną odpowiedzialnością
71	**Wuza 3** Spółka z ograniczoną odpowiedzialnością
72	**Wuza 4** Spółka z ograniczoną odpowiedzialnością
73	**Fraskata** Spółka z ograniczoną odpowiedzialnością
74	**Re Advisory Services** Spółka z ograniczoną odpowiedzialnością
75	**Re Commercial Services** Spółka z ograniczoną odpowiedzialnością
76	**Safe Invest** Spółka z ograniczoną odpowiedzialnością
77	**Ghelamco Polska** Spółka z ograniczoną odpowiedzialnością
78	**Agrimax** Spółka z ograniczoną odpowiedzialnością w likwidacji
79	**Agronut** Spółka z ograniczoną odpowiedzialnością w likwidacji
80	**Ecorol** Spółka z ograniczoną odpowiedzialnością w likwidacji
81	**Osney** Spółka z ograniczoną odpowiedzialnością
82	**Otter** Spółka z ograniczoną odpowiedzialnością
83	**Signal OS Tech** spółka z ograniczoną odpowiedzialnością
84	**Ghelamco Foksal** Spółka z ograniczoną odpowiedzialnością (dawniej: Ghelamco GP 5 Spółka z ograniczoną odpowiedzialnością Foksal S.K.A.)
85	**Groen Konstancin I** Spółka z ograniczoną odpowiedzialnością (dawniej: Ghelamco GP 1 Spółka z ograniczoną odpowiedzialnością Konstancin S.K.A.)
86	**Tilia Bis** Spółka z ograniczoną odpowiedzialnością
87	**Bliskie Piaseczno** Spółka z ograniczoną odpowiedzialnością (dawniej: Oaken Spółka z ograniczoną odpowiedzialnością Pattina S.K.A.)
88	Fundacja **Sztuka w Mieście**