

POLITYKA OCHRONY DANYCH OSOBOWYCH I BEZPIECZEŃSTWA

PRISTINE SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

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 spółce Pristine spółka z ograniczoną odpowiedzialnością z siedzibą w Warszawie pod adresem: ul. Leszczyńska 4/198, 00-339 Warszawa, wpisanej do rejestru przedsiębiorców Krajowego Rejestru Sądowego, prowadzonego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS 0000479921, NIP: 5252567967, REGON: 146915210 (dalej jako „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 L 119, s. 1).

3. Odpowiedzialny za:

a. wdrożenie i utrzymanie niniejszej Polityki oraz nadzór i monitorowanie jej przestrzegania jest Zarząd Spółki,

b. 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.

4. Skróty i definicje:

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

b. „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);

c. „Dane” oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu;

d. „Dane wrażliwe” oznaczają dane specjalne i dane karne;

e. „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;

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

g. „Dane dzieci” oznaczają dane osób poniżej 16. roku życia;

h. „Podmiot przetwarzający” oznacza podmiot, któremu Spółka powierzyła przetwarzanie danych osobowych (np. zewnętrzna księgowość);

i. „Profilowanie” oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

j. „Eksport danych” oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej;

k. „RCPD” lub „Rejestr” oznacza Rejestr Czynności Przetwarzania Danych Osobowych;

l. „Spółka” oznacza Pristine spółka z ograniczoną odpowiedzialnością z siedzibą w Warszawie pod adresem: ul. Leszczyńska 4/198, 00-339 Warszawa, wpisanej do rejestru przedsiębiorców Krajowego Rejestru Sądowego, prowadzonego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS 0000479921, NIP: 5252567967, REGON: 146915210.

5. Ochrona danych osobowych w Spółce – zasady ogólne

a. Filary ochrony danych osobowych w Spółce:

- i. Legalność – Spółka dba o ochronę prywatności i przetwarza dane zgodnie z prawem;
- ii. Bezpieczeństwo – Spółka zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie;
- iii. Prawa Jednostki – Spółka umożliwia osobom, których dane przetwarza, wykonywanie tych praw i prawa te realizuje;
- iv. Rozliczalność – Spółka dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

b. Zasady ochrony danych

Spółka przetwarza dane osobowe z poszanowaniem następujących zasad:

- i. w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
- ii. rzetelnie i uczciwie (rzetelność);
- iii. w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
- iv. w konkretnych celach i nie „na zapas” (minimalizacja);
- v. nie więcej niż potrzeba (adekwatność);
- vi. z dbałością o prawidłowość danych (prawidłowość);
- vii. nie dłużej niż potrzeba (czasowość);
- viii. zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

6. System ochrony danych

System ochrony danych w Spółce składa się z następujących elementów:

a. Inwentaryzacja danych. Spółka dokonuje identyfikacji zasobów danych osobowych w Spółce, w tym:

- i. przypadków przetwarzania danych specjalnych i danych karnych (dane wrażliwe);
- ii. przypadków przetwarzania danych osób, których Spółka nie identyfikuje (dane niezidentyfikowane);
- iii. przypadków przetwarzania danych dzieci;
- iv. profilowania;
- v. współadministrowania danymi.

b. Rejestr. Spółka opracowuje, prowadzi i utrzymuje Rejestr Czynności Danych osobowych w Spółce (Rejestr). Rejestr jest narzędziem rozliczania zgodności z ochroną danych w Spółce.

c. Podstawy prawne. Spółka identyfikuje oraz weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:

- i. utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikacją na odległość;
- ii. wskazuje uzasadnienie przypadków, gdy Spółka przetwarza dane na podstawie prawnie uzasadnionego interesu Spółki.

d. 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:

- i. Obowiązki informacyjne. Spółka przekazuje osobom prawem wymagane informacje przy zbieraniu ich danych osobowych oraz zapewnia udokumentowanie realizacji tych obowiązków;
- ii. 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;
- iii. Obsługa żądań. Spółka zapewnia odpowiednie procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO i udokumentowane;
- iv. 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.
- g. Przetwarzający. Spółka stosuje kryteria doboru 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.
- 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.

7. Inwentaryzacja

a. 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.

b. Dane niezidentyfikowane

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

c. 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.

d. Współadministrowanie

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

8. Rejestr Czynności Przetwarzania Danych („RCPD”)

a. 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 osobowych, czyli zasady rozliczalności.

b. Spółka prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.

c. Rejestr jest jednym z podstawowych narzędzi umożliwiających Spółce rozliczanie większości obowiązków ochrony danych.

d. 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 przetwarzających), (viii) informację o przekazaniu poza EU/EOG; (ix) ogólny opis technicznych i organizacyjnych środków ochrony danych.

9. Podstawy przetwarzania

- a. Spółka dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.
- b. 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.
- c. 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.).

10. Sposób obsługi praw jednostki i obowiązków informacyjnych

- a. Spółka dba o czytelność i styl przekazywania informacji i komunikacji z osobami, których dane przetwarza.
- b. 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.
- c. Spółka dba o dotrzymanie prawnych terminów realizacji obowiązków względem osób.
- d. Spółka wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.
- e. 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.
- f. Spółka dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

11. Obowiązki informacyjne

- a. Spółka określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.
- b. Spółka informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.
- c. Spółka informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.
- d. 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).
- e. 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).
- f. Spółka informuje osobę o planowanej zmianie celu przetwarzania danych.
- g. Spółka informuje osobę przed uchyleniem ograniczenia przetwarzania (w sytuacjach wskazanych w punkcie 13 i) poniżej).
- h. Spółka informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba, że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).
- i. Spółka informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.
- j. Spółka bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

12. Żądania osób

- a. 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.
- b. Nieprzetwarzanie. Spółka informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosi żądanie dotyczące jej praw.

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

d. 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.

e. 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.

f. 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.

g. 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.

h. Usunięcie danych. Na żądanie osoby, Spółka usuwa dane, gdy:

i. dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach;

ii. zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania;

iii. osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych;

iv. dane były przetwarzane niezgodnie z prawem;

v. konieczność usunięcia wynika z obowiązku prawnego. 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 osobowe, o potrzebie usunięcia danych i dostępu do nich. W przypadku usunięcia danych Spółka informuje osobę o odbiorcach danych, na żądanie tej osoby.

i. Ograniczenie przetwarzania. Spółka dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:

i. osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość;

ii. przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;

iii. Spółka nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;

iv. 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 uchynieniem ograniczenia przetwarzania. W przypadku ograniczenia przetwarzania danych Spółka informuje osobę o odbiorcach danych, na żądanie tej osoby.

j. 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.

k. 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.

l. Sprzeciw przy badaniach naukowych, historycznych lub celach statystycznych. Jeżeli Spółka prowadzi badania naukowe, historyczne lub przetwarza dane w celach statystycznych, osoba może wnieść umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania. Spółka uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

m. 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.

n. 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.

13. 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.

a. Minimalizacja zakresu

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

ii. Spółka dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.

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

b. Minimalizacja dostępu

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

ii. Spółka dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających.

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

c. Minimalizacja czasu

i. Spółka regularnie dokonuje przeglądu przetwarzanych danych osobowych 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.

ii. 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.

14. Bezpieczeństwo

a. Spółka zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Spółkę.

b. Spółka zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania – wewnątrz lub ze wsparciem podmiotów wyspecjalizowanych.

c. 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:

i. zabezpieczanie plików zawierających zbiory danych osobowych hasłami dostępu;

ii. 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 i ograniczanie dostępu do systemów informatycznych itp.);

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

d. Środki bezpieczeństwa

i. Spółka stosuje środki bezpieczeństwa adekwatne do rodzaju i ilości przetwarzanych danych osobowych

ii. Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa w Spółce.

e. 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.

f. Spółka opracowała i stosuje Instrukcję zarządzania systemami IT Spółki, która obowiązuje od 25 maja 2018 roku.

15. Przetwarzający

a. 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.

b. Każda umowa powierzenia przetwarzania danych zawierana przez Spółkę powinna spełniać wymagania określone w RODO.

c. Spółka rozlicza przetwarzających z wykorzystania podprzetwarzających, jak też z innych wymagań wynikających z Zasad powierzenia danych osobowych.

16. Eksport danych

Spółka rejestruje w Rejestrze przypadki eksportu danych, czyli przekazywania danych poza Europejski Obszar Gospodarczy (EOG w 2017 r. = Unia Europejska, Islandia, Lichtenstein i Norwegia).

17. Projektowanie prywatności

a. 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 osobowych oraz minimalizacji ich przetwarzania.

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