EBIS – POLITYKA OCHRONY DANYCH

Spis treści

I POSTANOWIENIA OGÓLNE....3
II OCHRONA DANYCH W SPÓŁCE....4
III INWENTARYZACJA....6
IV OBSŁUGI PRAW JEDNOSTKI....6
V OBOWIĄZKI INFORMACYJNE....7
VI MINIMALIZACJA....7
VI BEZPIECZEŃSTWO....8
VII PRZETWARZAJĄCY....9
VIII PROJEKTOWANIE PRYWATNOŚCI....10
IX POSTANOWIENIA KOŃCOWE....10

POLITYKA OCHRONY DANYCH

I
POSTANOWIENIA OGÓLNE

1. Niniejszy dokument zatytułowany „Polityka ochrony danych" (dalej jako „**Polityka**") ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych w EBIS spółka z ograniczoną odpowiedzialnością z siedzibą w Krakowie.

2. Niniejsza 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).

3. Polityka zawiera:

3.1 opis zasad ochrony danych obowiązujących w Spółce;

3.2 odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach);

4. Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest zarząd Spółki. Spółka zapewnia zgodność postępowania kontrahentów Spółki z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez Spółkę.

5. Definicje:

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

5.2 **„Dane wrażliwe"** 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.

5.3 **„Eksport danych"** oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej.

5.4 **„Osoba"** oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.

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

5.6 **„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.

5.7 **„Przetwarzający"** oznacza organizację lub osobę, której Spółka powierzyła przetwarzanie danych osobowych (np. usługodawca IT, zewnętrzna księgowość).

5.8 **„RODO"** oznacza rozporządzenie 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).

5.9 **„Spółka"** oznacza EBIS spółka z ograniczoną odpowiedzialnością z siedzibą w Krakowie, ul. Samuela Lindego 1C, 30-148 Kraków, wpisaną do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla Krakowa-Śródmieścia w Krakowie, Wydział XI Gospodarczy KRS, pod numerem 0000459760, NIP: 6762464669, REGON: 1228439070, kapitał zakładowy: 51.000,00 zł.

II
OCHRONA DANYCH W SPÓŁCE

6. Filarami ochrony danych w Spółce są:

6.1 **Legalność** – Spółka dba o ochronę prywatności i przetwarza dane zgodnie z prawem.

6.2 **Bezpieczeństwo** – Spółka zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.

6.3 **Prawa Jednostki** – Spółka umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.

6.4 **Rozliczalność** – Spółka dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

7. Spółka przetwarza dane osobowe z poszanowaniem następujących zasad:

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

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

7.3 w sposób przejrzysty dla osoby, której dane dotyczą (**transparentność**);

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

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

7.6 z należytą dbałością o prawidłowość danych (**prawidłowość**);

7.7 nie dłużej niż jest to konieczne (**czasowość**);

7.8 zapewniając odpowiednie bezpieczeństwo danych (**bezpieczeństwo).**

8. System ochrony danych w Spółce składa się z następujących elementów:

8.1 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 danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków.

(b) Możliwość wykonania żądań. Spółka weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających.

(c) Obsługa żądań. Spółka zapewnia odpowiednie nakłady i procedury, aby żądania Osób były realizowane w terminach i w sposób wymagany RODO i dokumentowane.

(d) Zawiadamianie o naruszeniach. Spółka stosuje procedury pozwalające na ustalenie konieczności zawiadomienia Osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

8.2 Minimalizacja. Spółka posiada zasady i metody zarządzania minimalizacją (privacy by default), a w tym:

(a) zasady zarządzania adekwatnością danych;

(b) zasady reglamentacji i zarządzania dostępem do danych;

(c) zasady zarządzania okresem przechowywania danych i weryfikacji dalszej przydatności;

8.3 Bezpieczeństwo. Spółka zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:

(a) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;

(b) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności Osób jest wysokie;

(c) dostosowuje środki ochrony danych do ustalonego ryzyka;

(d) posiada system zarządzania bezpieczeństwem informacji;

(e) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych – zarządza incydentami.

8.4 Przetwarzający. Spółka posiada zasady doboru przetwarzających dane na rzecz Spółki, wymogów co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia.

8.5 Eksport danych. Spółka posiada zasady weryfikacji, czy Spółka nie przekazuje danych do państw trzecich lub do organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków takiego przekazywania, jeśli ma ono miejsce.

8.6 Privacy by design. Spółka zarządza zmianami mającymi wpływ na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji w Spółce uwzględniają

konieczność oceny wpływu zmiany na ochronę danych, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.

8.7 Przetwarzanie transgraniczne. Spółka posiada zasady weryfikacji, kiedy zachodzą przypadki przetwarzania transgranicznego oraz zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO.

III
INWENTARYZACJA

9. Spółka dokonuje identyfikacji zasobów danych osobowych w Spółce, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych (inwentaryzacja).

9.1 **Dane wrażliwe.** Spółka identyfikuje przypadki, w których przetwarza lub może przetwarzać dane wrażliwe 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.

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

9.3 **Profilowanie.** Spółka identyfikuje przypadki, w których dokonuje profilowania przetwarzanych 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.

9.4 **Współadministrowanie.** Spółka identyfikuje przypadki współadministrowania danymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami.

IV
OBSŁUGI PRAW JEDNOSTKI

10. Spółka dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.

10.1 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.

10.2 Spółka dba o dotrzymywanie prawnych terminów realizacji obowiązków względem Osób.

10.3 Spółka wprowadza adekwatne metody identyfikacji i uwierzytelniania Osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.

10.4 W celu realizacji praw jednostki Spółka zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych Osób przetwarzane przez Spółkę, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany.

10.5 Spółka dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań Osób.

10.6 Spółka posiada procedurę realizowania żądań Osób trzecich.

V
OBOWIĄZKI INFORMACYJNE

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

11.1 Spółka informuje osobę o:

(a) przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby;

(b) przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby;

(c) przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej;

(d) planowanej zmianie celu przetwarzania danych;

(e) sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe);

(f) prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.

11.2 Spółka określa sposób informowania Osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym).

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

VI
MINIMALIZACJA

12. 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.

12.1 **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*).

12.2 **Minimalizacja dostępu:**

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

(b) Spółka stosuje kontrolę dostępu fizycznego.

(c) Spółka dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról Osób, oraz zmianach podmiotów przetwarzających.

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

(e) Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w procedurach bezpieczeństwa fizycznego i bezpieczeństwa informacji Spółki.

12.3 **Minimalizacja czasu:**

(a) Spółka wdraża mechanizmy kontroli cyklu życia danych osobowych w Spółce, w tym 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 produkcyjnych Spółki, jak też z akt podręcznych i głównych. 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 wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

VI
BEZPIECZEŃSTWO

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

13.1 Spółka przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:

(a) Spółka zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania – wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.

(b) Spółka kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.

(c) 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 osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

(d) Spółka ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. Spółka ustala przydatność i stosuje takie środki i podejście jak:

(i) pseudonimizacja,

(ii) szyfrowanie danych osobowych,

(iii) inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,

(iv) 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.

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

13.3 Spółka stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych. Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa w Spółce i są bliżej opisane w procedurach przyjętych przez Spółkę dla tych obszarów.

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

VII
PRZETWARZAJĄCY

14. Spółka posiada zasady doboru i weryfikacji przetwarzających dane na rzecz Spółki opracowane 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.

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

VIII
PROJEKTOWANIE PRYWATNOŚCI

16. Spółka zarządza zmianą mającą wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania.

17. W tym celu zasady prowadzenia projektów i inwestycji przez Spółkę odwołują się do zasad bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę danych, uwzględnienia i zaprojektowana bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub inwestycji.

IX
POSTANOWIENIA KOŃCOWE

18. Niniejsza Polityka obowiązuje od 01.05.2018 r.