Polityka ochrony danych osobowych

§1

[postanowienia ogólne]

1. Niniejszy dokument (dalej: Polityka) jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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).

2. Polityka zawiera opis zasad ochrony danych obowiązujących w firmie Agnieszka Cieplik z siedzibą przy ul. Aroniowej 18, 62-090 Bytkowo, NIP 783 158 05 35

3. Administratorem danych osobowych jest Agnieszka Cieplik z siedzibą przy ul. Aroniowej 18, 62-090 Bytkowo,

NIP 783 158 05 35

4. Odpowiedzialna za wdrożenie i utrzymanie niniejszej Polityki jest Agnieszka Cieplik.

5. Za nadzór i monitorowanie przestrzegania Polityki odpowiada Inspektor Ochrony Danych (dalej: IOD). Kontakt: a.cieplik@target-szkolenia.pl

6. Firma zapewnia zgodność postępowania kontrahentów Firmy z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez Firmę.

§2

[skróty i definicje]

1. Polityka oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu.

2. RODO oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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).

3. Dane oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu.

4. Dane szczególnych kategorii 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, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

5. Dane karne oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa.

6. Dane dzieci oznaczają dane osób poniżej 16 roku życia.

7. Osoba oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.

8. Pomiot przetwarzający oznacza organizację lub osobę, której Spółka powierzyła przetwarzanie danych osobowych.

9. 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.

10. Eksport danych oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej.

11. RCPD lub Rejestr oznacza Rejestr Czynności Przetwarzania Danych Osobowych.

§3

[zasady ochrony danych osobowych w Spółce]

1. Administrator danych zobowiązany jest zastosować środki techniczne
i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

2. Administrator danych zobowiązany jest do zapewnienia, aby dane osobowe były:

1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);

2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami („ograniczenie celu”);

3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);

4) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe
w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);

5) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane („ograniczenie przechowywania”);

6) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”).

3. Administrator danych wyznacza IOD w przypadkach, w których RODO wprowadza taki obowiązek, lub w sytuacji, gdy sam uzna to za konieczne.

4. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora danych. Osoby te są zobowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczania.

5. Administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

6. IOD powołany przez Firmę odpowiada za bezpieczeństwo systemu informatycznego, w którym przetwarzane są dane osobowe.

7. Do obowiązków IOD należy:

1) Wykonywanie zadań określonych w RODO, a w szczególności w przepisach art. 39 ust. 1 RODO,

2) nadzór nad przestrzeganiem Polityki bezpieczeństwa i Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,

3) nadzór i kontrola systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych,

4) nadzór nad właściwym zabezpieczeniem sprzętu oraz pomieszczeń, w których przetwarzane są dane osobowe,

5) nadzór nad wykorzystanym w placówce oprogramowaniem oraz jego legalnością,

6) przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe,

7) podejmowanie odpowiednich działań w celu właściwego zabezpieczania danych,

8) badanie ewentualnych naruszeń w systemie zabezpieczeń danych osobowych,

9) podejmowanie decyzji o instalowaniu nowych urządzeń oraz oprogramowania wykorzystanego do przetwarzania danych osobowych,

10) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, zawierających dane osobowe,

11) definiowanie haseł dostępu,

12) aktualizowanie oprogramowania antywirusowego i innego, chyba, że aktualizacje te wykonywane są automatycznie,

13) wykonywanie kopii zapasowych, ich przechowywanie oraz okresowe sprawdzanie pod kątem ich dalszej przydatności,

14) wdrożenie wewnętrznych szkoleń z zakresu przepisów dotyczących ochrony danych osobowych oraz środków technicznych i organizacyjnych przy przetwarzaniu danych w systemach informatycznych,

15) sporządzanie raportów z naruszenia bezpieczeństwa systemu informatycznego oraz systemu przechowywania i zabezpieczenia danych osobowych zgromadzonych i utrwalonych w innej formie, niż elektroniczna,

16) zapewnienie ochrony i bezpieczeństwa danych osobowych znajdujących się w systemie informatycznym Spółki oraz w tradycyjnych zbiorach danych, ze szczególnym uwzględnieniem dokumentacji medycznej,

17) niezwłoczne informowanie Administratora danych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,

18) podejmowanie, zgodnie z Polityką, stosownych działań w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym oraz danych osobowych zgromadzonych i utrwalonych w innej formie, niż elektroniczna,

19) zapewnienie fizycznego bezpieczeństwa systemu informatycznego oraz systemu przechowywania i zabezpieczenia danych osobowych zgromadzonych i utrwalonych w innej formie, niż elektroniczna,

20) zapewnienie bezpieczeństwa funkcjonowania wszystkich urządzeń pracujących w systemie,

21) zapewnienie dostępu do systemu wyłącznie dla osób uprawnionych.

§4

[system ochrony danych osobowych]

1. Spółka dokonuje identyfikacji zasobów danych osobowych, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych, w tym:

1) przypadków przetwarzania danych szczególnych kategorii i danych karnych,

2) przypadków przetwarzania danych osób, których spółka nie identyfikuje,

3) przypadków przetwarzania danych dzieci,

4) profilowania,

5) współadministrowania danymi.

2. Firma opracowuje, prowadzi i utrzymuje Rejestr Czynności Przetwarzania Danych Osobowych. Rejestr jest narzędziem rozliczania zgodności z ochroną danych w Firmie.

3. Firma zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:

1) utrzymuje system zarządzania zgodami na przetwarzanie danych
i komunikację na odległość,

2) inwentaryzuje i uszczegóławia przypadki, gdy Firma przetwarza dane na podstawie prawnie uzasadnionego interesu Firmy.

4. Firma spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane
w tym zakresie żądania, a w szczególności:

1) przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków,

2) weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających,

3) zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany przez RODO
i odpowiednio dokumentowane,

4) stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

5. Firma stosuje zasady i metody zarządzania minimalizacją (privacy by deflaut), a w tym:

1) zasady zarządzania adekwatnością danych,

2) zasady reglamentacji i zarządzania dostępem do danych,

3) zasady zarządzania okresem przechowywania danych i weryfikacji dalszej przydatności.

6. Firma zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:

1) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii,

2) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie,

3) dostosowuje środki ochrony danych do ustalonego ryzyka,

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

7. Firma posiada zasady doboru przetwarzających dane na rzecz Firmy, wymogów co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonania umów powierzenia.

8. Spółka stosuje zasady weryfikacji, czy nie przekazuje danych do państw trzecich (poza UE, Norwegię, Lichtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnia zgodne z prawem warunki przekazania, jeśli ma ono miejsce.

9. Firma zarządza zmianami wpływającymi na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji w Firmie uwzględniają konieczność oceny wpływu zmiany na ochronę danych, analizę ryzyka, zapewnienie prywatności (a w tym celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.

10. Firma stosuje zasady weryfikacji, kiedy zachodzą przypadki przetwarzania transgranicznego oraz zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO.

§5

[inwentaryzacja]

1. Firma identyfikuje przypadki, w których:

1) przetwarza lub może przetwarzać dane szczególnych kategorii lub dane karne, oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania takich danych. W razie zidentyfikowania przypadków przetwarzania danych szczególnych kategorii lub danych karnych Spółka postępuje zgodnie z przyjętymi zasadami w tym zakresie,

2) przetwarza lub może przetwarzać dane niezidentyfikowane
i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane,

3) dokonuje profilowania przetwarzanych danych i utrzymuje mechanizmy zapewniające zgodność tego procesu z prawem.
W razie zidentyfikowania przypadków profilowania
i zautomatyzowanego podejmowania decyzji Firma postępuje zgodnie z przyjętymi zasadami w tym zakresie,

4) współadministruje danymi i postępuje w tym zakresie zgodnie
z przyjętymi zasadami.

§6

[Rejestr Czynności Przetwarzania Danych]

1. Rejestr Czynności Przetwarzania Danych 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.

2. Firma prowadzi Rejestr, w którym inwentaryzuje i monitoruje sposób,
w jaki wykorzystuje dane osobowe.

3. Rejestr jest jednym z podstawowych narzędzi umożliwiających Firmie rozliczanie większości obowiązków ochrony danych.

4. Firma dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.

5. Wskazując w dokumentach ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne, uzasadniony cel spółki), Firma dookreśla podstawę w precyzyjny i czytelny sposób.

6. Firma wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności.

§7

[sposób obsługi praw jednostki i obowiązków informacyjnych]

1. Firma dba o czytelność i styl przekazywanych informacji i komunikacji
z osobami, których dane przetwarza.

2. Firma ułatwia osobom korzystanie z ich praw poprzez różne działania, tj.: zamieszczanie na stronie internetowej Firmy informacji lub linków do informacji o prawach osób, sposobie skorzystania z nich w Firmie,
w tym wymaganiach dotyczących identyfikacji, metodach kontaktu ze Spółką w tym celu, ewentualnym cenniku żądań „dodatkowych” itp.

3. Firma dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.

4. Firma wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.

5. W celu realizacji praw jednostki Firma zapewnia procedury
i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Firmę, zintegrować te dane, wprowadzać do nich zmiany i usuwać je w sposób zintegrowany.

6. Firma dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

§8

[żądania osób]

1. Realizując prawa osób, których dane dotyczą, Firma 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, Firma może się zwrócić do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

2. Firma informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.

3. Firma informuje osobę, w ciągu miesiąca od otrzymania żądania,
o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.

4. Na żądanie osoby dotyczące dostępu do jej danych Firma informuje osobę, czy przetwarza jej dane, oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO, a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych, z zastrzeżeniem, że kopii danych wydanej w wykonaniu prawa dostępu do danych Firma nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.

§9

[minimalizacja]

1. Firma dba o minimalizację przetwarzania danych pod kątem:

1) adekwatności danych do celów,

2) dostępu do danych,

3) czasu przechowywania danych.

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

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

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

5. Firma stosuje ograniczenia dostępu do danych osobowych:

1) prawne (zobowiązania do poufności, zakresy upoważnień),

2) fizyczne (strefy dostępu, zamykanie pomieszczeń),

3) logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych w których rezydują dane osobowe).

6. Firma stosuje kontrolę dostępu fizycznego.

7. Firma dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób oraz zmianach podmiotów przetwarzających.

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

9. Firma wdraża mechanizmy kontroli cyklu życia danych osobowych w Firmie, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze.

10. Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu, są usuwane z systemów produkcyjnych Firmy, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Spółkę. Zasady archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

§11

[bezpieczeństwo]

1. Firma zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Firmę.

2. Firma przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:

1) Firma zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania – wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych,

2) Firma kategoryzuje dane oraz czynności przetwarzania pod katem ryzyka, które przedstawiają.

3) Firma przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Firma 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,

§12

[eksport danych]

1. Firma stosuje zasady doboru i weryfikacji przetwarzających dane na rzecz Firmy 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 Firmie.