POLITYKA OCHRONY DANYCH OSOBOWYCH

I. Niniejszy dokument zatytułowany „Polityka Ochrony Danych Osobowych” (dalej określany jako Polityka) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony DO w SPORTKONSULTING Spółka z ograniczoną odpowiedzialnością (dalej określany jako Firma).
Niniejsza Polityka jest polityką ochrony Danych Osobowych (dalej: DO) 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 DO 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) i przepisami krajowymi (dalej łącznie: RODO).
II. Polityka zawiera:
1. Opis zasad ochrony DO obowiązujących w Firmie.
2. Odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony DO wymagających doprecyzowania w odrębnych dokumentach).
III. Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest Zarząd Firmy, a w ramach Zarządu:
1. Ryszard Szul, któremu powierzono nadzór nad obszarem ochrony DO.
2. Osoba wyznaczona przez Firmę do zapewnienia zgodności z ochrona DO.
Za nadzór i monitorowanie przestrzegania Polityki odpowiadają:
3. Inspektor Ochrony Danych.
Za stosowanie niniejszej Polityki odpowiedzialni są:
4. Firma.
5. Komórka organizacyjna odpowiedzialna za obszar bezpieczeństwa informacji.
6. Komórki organizacyjne przetwarzające DO.
7. Personel Firmy.
8.
Firma zapewni zgodność postępowania kontrahentów Firmy z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im DO przez Firmę.
IV. Skróty i definicje:
1. Polityka oznacza niniejszą Politykę ochrony DO, o ile co innego nie wynika wyraźnie z kontekstu.
2. RODO oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem DO 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. Dane oznaczają DO, o ile co innego nie wynika wyraźnie z kontekstu.
4. Dane wrażliwe oznaczają dane specjalne i dane karne.
5. Dane specjalne oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. DO 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.
6. Dane karne oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa.
7. Dane dzieci oznaczają dane osób poniżej 16. roku życia.
8. Osoba oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.
9. Podmiot przetwarzający oznacza organizację lub osobę, której Firma powierzyła przetwarzanie DO (np. usługodawca IT, zewnętrzna księgowość).
10. Profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania DO, które polega na wykorzystaniu DO 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.
11. Eksport danych oznacza przekazanie DO do państwa trzeciego lub organizacji międzynarodowej.
12. IOD lub Inspektor oznacza Inspektora Ochrony DO.
13. RCPD lub Rejestr oznacza Rejestr Czynności Przetwarzania DO.
14. Firma oznacza podmiot wymieniony w preambule.
V. Ochrona DO – zasady ogólne
1. Filary ochrony DO:
1. Legalność − Firma dba o ochronę prywatności i przetwarza dane zgodnie z prawem.
2. Bezpieczeństwo − Firma zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.
3. Prawa Jednostki − Firma umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
4. Rozliczalność − Firma dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.
2. Zasady ochrony danych.
Firma przetwarza DO z poszanowaniem następujących zasad:
1. W oparciu o podstawę prawną i zgodnie z prawem (legalizm).
2. Rzetelnie i uczciwie (rzetelność).
3. W sposób przejrzysty dla osoby, której dane dotyczą (transparentność)
4. W konkretnych celach i nie „na zapas” (minimalizacja).
5. Nie więcej niż potrzeba (adekwatność).
6. Z dbałością o prawidłowość danych (prawidłowość).
7. Nie dłużej niż potrzeba (czasowość).
8. Zapewniając odpowiednie bezpieczeństwo DO (bezpieczeństwo).

3. System ochrony DO
System ochrony DO w Firmie składa się z następujących elementów:
1. Inwentaryzacja danych. Firma dokonuje identyfikacji zasobów DO w Firmie, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych (inwentaryzacja), w tym:
1. Przypadków przetwarzania danych specjalnych i danych „kryminalnych” (dane wrażliwe).
2. Przypadków przetwarzania danych osób, których Firma nie identyfikuje (dane niezidentyfikowane/UFO).
3. Przypadków przetwarzania danych dzieci.
4. Profilowania.

5. Współadministrowania danymi.
2. Rejestr. Firma opracowuje, prowadzi i utrzymuje Rejestr Czynności DO w Firmie (Rejestr). Rejestr jest narzędziem rozliczania zgodności z ochroną danych w Firmie. Rejestr zostanie zaprowadzony dopiero w przypadku gdy Firma przekroczy limity wyrażone w RODO.
3. Podstawy prawne. 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 uzasadnienie przypadków, gdy Firma przetwarza dane na podstawie prawnie uzasadnionego interesu Firmy.
4. Obsługa praw jednostki. Firma spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
Obowiązki informacyjne. Firma przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków.
1. Możliwość wykonania żądań. Firma weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających.
2. Obsługa żądań. Firma zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO i dokumentowane.
3. Zawiadamianie o naruszeniach. Firma stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.
5. Minimalizacja. Firma posiada zasady i metody zarządzania minimalizacją (privacy by default), 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. Bezpieczeństwo. Firma zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:
1. Przeprowadza analizy ryzyka dla czynności przetwarzania DO lub ich kategorii.
2. Przeprowadza oceny skutków dla ochrony DO tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie.
3. Dostosowuje środki ochrony danych do ustalonego ryzyka.
4. Posiada system zarządzania bezpieczeństwem informacji.
5. Stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych − zarządza incydentami.
7. Przetwarzający. Firma posiada zasady doboru przetwarzających dane na rzecz Firmy, wymogów co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia.
8. Eksport danych. Firma posiada zasady weryfikacji, czy Firma nie przekazuje danych do państw trzecich (czyli poza UE, Norwegię, Lichtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków takiego przekazywania, w przypadku gdy ma ono miejsce.
9. Privacy by design. Firma zarządza zmianami mającymi wpływ na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji w Firmie 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.
10. Przetwarzanie transgraniczne. Firma posiada zasady weryfikacji, kiedy zachodzą przypadki przetwarzania transgranicznego oraz zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO.
VI. Inwentaryzacja
1. Dane wrażliwe - Firma 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, Firma postępuje zgodnie z przyjętymi zasadami w tym zakresie.
2. Dane niezidentyfikowane - Firma identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane.
3. Profilowanie - Firma 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, Firma postępuje zgodnie z przyjętymi zasadami w tym zakresie.
4. Współadministrowanie - Firma identyfikuje przypadki współadministrowania danymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami.
VII. Rejestr Czynności Przetwarzania Danych – część nieaktywna do momentu wyznaczonego przepisami.
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 DO, czyli zasady rozliczalności.
2. Firma prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje DO.
3. Rejestr jest jednym z podstawowych narzędzi umożliwiających Firmie rozliczanie większości obowiązków ochrony danych.
4. W Rejestrze, dla każdej czynności przetwarzania danych, którą Firma uznała za odrębną dla potrzeb Rejestru, Firma odnotowuje co najmniej:
1. Nazwę czynności,
2. Cel przetwarzania,
3. Opis kategorii osób,

4. Opis kategorii danych,
5. Podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu Firmy, jeśli podstawą jest uzasadniony interes,
6. Sposób zbierania danych,
7. Opis kategorii odbiorców danych (w tym przetwarzających),
8. Informację o przekazaniu poza EU/EOG,
9. Ogólny opis technicznych i organizacyjnych środków ochrony danych.
5. Wzór Rejestru stanowi Załącznik nr 1 do Polityki – „Wzór Rejestru Czynności Przetwarzania Danych”. Wzór Rejestru zawiera także kolumny nieobowiązkowe. W kolumnach nieobowiązkowych Firma rejestruje informacje w miarę potrzeb i możliwości, z

uwzględnieniem tego, że pełniejsza treść Rejestru ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej.
VIII. Podstawy przetwarzania.
1. Firma dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.
2. Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel Firmy) Firma 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.
3. 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 (email, telefon, sms, in.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).
4. Kierownik komórki organizacyjnej Firmy ma obowiązek znać podstawy prawne, na jakich komórka przez niego kierowana dokonuje konkretnych czynności przetwarzania DO. Jeżeli podstawą jest uzasadniony interes Firmy, kierownik komórki ma obowiązek znać konkretny realizowany przetwarzaniem interes Firmy.
IX. 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, w tym: zamieszczenie na stronie internetowej Firmy informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich w Firmie, w tym wymaganiach dotyczących identyfikacji, metodach kontaktu ze Firmą 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 w sposób zintegrowany,
6. Firma dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.
X. Obowiązki informacyjne.
1. Firma określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.
2. Firma informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.
3. Firma informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.
4. Firma informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej.
5. Firma określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym).
6. Firma informuje osobę o planowanej zmianie celu przetwarzania danych.
7. Firma informuje osobę przed uchyleniem ograniczenia przetwarzania.
8. Firma informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).
9. Firma informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.
10. Firma bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony DO, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.
XI. Żądania osób
1. Prawa osób trzecich. 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 (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnicę handlową, dobra osobiste itp.), Firma może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.
2. Nieprzetwarzanie. Firma informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.
3. Odmowa. Firma informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.
4. Dostęp do danych. 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 (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, 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.
5. Kopie danych. Na żądanie Firma wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Firma wprowadza i utrzymuje cennik kopii danych, zgodnie z którym pobiera opłaty za kolejne kopie danych. Cena kopii danych skalkulowana jest w oparciu o oszacowany jednostkowy koszt obsługi żądania wydania kopii danych.
6. Sprostowanie danych. Firma dokonuje sprostowania nieprawidłowych danych na żądanie osoby. Firma ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Firma informuje osobę o odbiorcach danych, na żądanie tej osoby.
7. Uzupełnienie danych. Firma uzupełnia i aktualizuje dane na żądanie osoby. Firma ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. Firma nie musi przetwarzać danych, które są Firmie zbędne). Firma

może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Firmę procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.
8. Usunięcie danych. Na żądanie osoby, Firma usuwa dane, gdy:
1. Dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,
2. Zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
3. Osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
4. Dane były przetwarzane niezgodnie z prawem,
5. Konieczność usunięcia wynika z obowiązku prawnego,
6. 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).

Firma 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 Firmę, Firma podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te DO, o potrzebie usunięcia danych i dostępu do nich.
W przypadku usunięcia danych Firma informuje osobę o odbiorcach danych, na żądanie tej osoby.
9. Ograniczenie przetwarzania. Firma dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:
1. Osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,
2. Przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu DO, żądając w zamian ograniczenia ich wykorzystywania,
3. Firma nie potrzebuje już DO, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
4. Osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Firmy zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.
W trakcie ograniczenia przetwarzania Firma 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.
Firma informuje osobę przed uchyleniem ograniczenia przetwarzania.
W przypadku ograniczenia przetwarzania danych Firma informuje osobę o odbiorcach danych, na żądanie tej osoby.
10. Przenoszenie danych. Na żądanie osoby Firma wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Firmie, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Firmy.
11. Sprzeciw w szczególnej sytuacji. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Firmę w oparciu o uzasadniony interes Firmy lub o powierzone Firmie zadanie w interesie publicznym, Firma uwzględni sprzeciw, o ile nie zachodzą po stronie Firmy ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.
12. Sprzeciw przy badaniach naukowych, historycznych lub celach statystycznych. Jeżeli Firma prowadzi badania naukowe, historyczne lub przetwarza dane w celach statystycznych, osoba może wnieść umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania. Firma uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.
13. Sprzeciw względem marketingu bezpośredniego. Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Firmę na potrzeby marketingu bezpośredniego (w tym ewentualnie profilowania), Firma uwzględni sprzeciw i zaprzestanie takiego przetwarzania.
14. Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu. Jeżeli Firma 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, Firma zapewnia możliwość odwołania się do interwencji i decyzji człowieka po stronie Firmy, chyba że taka automatyczna decyzja:
1. jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a Firmą.
2. jest wprost dozwolona przepisami prawa.
3. opiera się o wyraźną zgodę odwołującej osoby.
XII. Minimalizacja.
Firma dba o minimalizację przetwarzania danych pod kątem:
1. adekwatności danych do celów (ilości danych i zakresu przetwarzania),
2. dostępu do danych,
3. czasu przechowywania danych.
1. Minimalizacja zakresu.
Firma zweryfikowała zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO.
Firma dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.
Firma przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (privacy by design).
2. Minimalizacja dostępu.
Firma stosuje ograniczenia dostępu do DO: prawne (zobowiązania do poufności, zakresy upoważnień), fizyczne (strefy dostępu, zamykanie pomieszczeń) i logiczne (ograniczenia uprawnień do systemów przetwarzających DO i zasobów sieciowych, w których rezydują DO).
Firma stosuje kontrolę dostępu fizycznego.
Firma dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających.
Firma dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.
Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w procedurach bezpieczeństwa fizycznego i bezpieczeństwa informacji Firmy.
3. Minimalizacja czasu.
Firma wdraża mechanizmy kontroli cyklu życia DO w Firmie, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze.

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 Firmę. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.
XIII. Bezpieczeństwo.
Firma zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania DO przez Firmę.
1. Analizy ryzyka i adekwatności środków bezpieczeństwa.
Firma przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa DO. 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 kątem 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 DO uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.
4. Firma ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym Firma ustala przydatność i stosuje takie środki i podejście jak:
1. Pseudonimizacja.
2. Szyfrowanie DO.
3. Inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania.
4. Środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności DO i dostępu do nich w razie incydentu fizycznego lub technicznego.
2. Oceny skutków dla ochrony danych.
Firma dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony DO tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.
Firma stosuje metodykę oceny skutków przyjętą w Firmie.
3. Środki bezpieczeństwa.
Firma stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych.
Środki bezpieczeństwa DO stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa w Firmie i są bliżej opisane w procedurach przyjętych przez Firmę dla tych obszarów.
4. Zgłaszanie naruszeń
Firma stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia.
XIV. Przetwarzający.
Firma posiada 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.
Firma przyjęła minimalne wymagania co do umowy powierzenia przetwarzania danych stanowiące Załącznik nr 2 do Polityki – „Wzór umowy powierzenia przetwarzania danych".
Firma rozlicza przetwarzających z wykorzystania podprzetwarzających, jak też z innych wymagań wynikających z Zasad powierzenia DO.
XV. Eksport danych.
Firma rejestruje w Rejestrze przypadki eksportu danych, czyli przekazywania danych poza Europejski Obszar Gospodarczy (EOG w 2018 r. = Unia Europejska, Islandia, Lichtenstein i Norwegia).
Aby uniknąć sytuacji nieautoryzowanego eksportu danych w szczególności w związku z wykorzystaniem publicznie dostępnych usług chmurowych (shadow IT), Firma okresowo weryfikuje zachowania użytkowników oraz w miarę możliwości udostępnia zgodne z prawem ochrony danych rozwiązania równoważne.
XVI. Projektowanie prywatności.
Firma zarządza zmianą mającą wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa DO oraz minimalizacji ich przetwarzania.
W tym celu zasady prowadzenia projektów i inwestycji przez Firmę odwołują się do zasad bezpieczeństwa DO i minimalizacji, wymagając oceny wpływu na prywatność i ochronę danych, uwzględnienia i zaprojektowana bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub inwestycji.
XVII. Postanowienia końcowe.
Niniejsza Polityka wchodzi w życie z dniem 20.12.2021 r.