

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:

1) opis zasad ochrony danych obowiązujących w Auto-Mes-Con Spółka z ograniczoną odpowiedzialnością z siedzibą w Pławniowicach, ul. Nowa 14, 44-171 Pławniowice, wpisaną do Rejestru Przedsiębiorców KRS prowadzonego przez Sąd Rejonowy dla Głiwic, , X Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS: 0000317255, o kapitale zakładowym w wysokości 55.000,00 zł, (dalej: Spółka),

2) odwołania do załączników uszczegóławiających, a w szczególności procedur lub instrukcji dotyczących poszczególnych obszarów z zakresu ochrony danych osobowych.

3. Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest Pan Piotr Świszcz – Prezes Zarządu Spółki.

4. Spółka zapewnia zgodność postępowania kontrahentów Spółki z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez Spółkę.

§2

[skrót 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 uchylecia 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. Ochrona danych osobowych w Spółce opiera się o następujących filarach:

- 1) Legalizm – Spółka dba o ochronę prywatności i przetwarza dane zgodnie z prawem,
- 2) Bezpieczeństwo – Spółka zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stałe działania w tym zakresie,
- 3) Prawa Jednostki – Spółka umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje,
- 4) Rozliczalność – Spółka dokumentuje to, w jaki sposób przetwarza dane osobowe, aby w każdej chwili móc wykazać przed organami kontroli zgodność procedur z RODO.

2. Spółka przetwarza dane osobowe 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 danych (bezpieczeństwo).

§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. Spółka opracowuje, prowadzi i utrzymuje Rejestr Czynności Przetwarzania Danych Osobowych. Rejestr jest narzędziem rozliczania zgodności z ochroną danych w Spółce.

3. Spółka 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 Spółka przetwarza dane na podstawie prawnie uzasadnionego interesu Spółki.

4. Spółka 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. Spółka stosuje 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. Spółka 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. Spółka posiada zasady doboru przetwarzających dane na rzecz Spółki, 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. Spółka zarządza zmianami wpływającymi na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji w Spółce 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. Spółka stosuje zasady weryfikacji, kiedy zachodzą przypadki przetwarzania transgranicznego oraz zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO.

§5

[inwentaryzacja]

1. Spółka 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 Spółka 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. Spółka prowadzi Rejestr, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.

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

4. Spółka 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), Spółka dookreśla podstawę w precyzyjny i czytelny sposób.

6. 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 oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności.

§7

[sposób obsługi praw jednostki i obowiązków informacyjnych]

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

2. Spółka ułatwia osobom korzystanie z ich praw poprzez różne działania, tj.: zamieszczanie na stronie internetowej Spółki informacji lub 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.

3. Spółka dba o dotrzymanie prawnych terminów realizacji obowiązków względem osób.

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

5. 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 je w sposób zintegrowany.

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

§8

[obowiązki informacyjne]

1. Spółka określa zgodnie z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.

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

3. Spółka informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych tej osoby.

4. Spółka informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej.

5. Spółka określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam, gdzie to jest możliwe.

6. Spółka informuje osobę o planowanej zmianie celu przetwarzania danych.

7. Spółka informuje osobę przed uchyleniem ograniczenia przetwarzania.

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

9. Spółka informuje osobę o prawie sprzeciwu względem przetwarzania danych przy pierwszym kontakcie z tą osobą.

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

§9

[żądania osób]

1. 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, Spółka może się zwrócić do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

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

3. Spółka 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 Spółka 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 Spółka nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.

5. Na żądanie Spółka wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Spółka wprowadza i utrzymuje cennik kopii danych, zgodnie z którym pobiera opłaty za kolejne kopie danych. Cena kopii danych skalkulowana jest na podstawie oszacowanego jednostkowego kosztu obsługi żądania wydania kopii danych.

6. 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.

7. Spółka uzupełnia i aktualizuje dane na żądanie osoby. Spółka ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych. Spółka może polegać na oświadczeniu osoby co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Spółkę procedur, prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

8. Na żądanie osoby Spółka usuwa dane, gdy:

1) dane nie są niezbędne do celów, dla których zostały zebrane, ani przetwarzane w innych zgodnych z prawem 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.

9. 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.

10. 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.

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

12. Spółka 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 danych osobowych,