

## **POLITYKA OCHRONY DANYCH OSOBOWYCH**

**Midorino Judo Teresa Klaczyńska**



### **§1. Polityka Ochrony Danych Osobowych**

Niniejszy dokument zatytułowany „Polityka ochrony danych osobowych” (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.

Wykaz procedur, polityk oraz instrukcji regulujących bezpieczne oraz zgodne z prawem przetwarzanie danych osobowych w Midorino Judo Teresa Klaczyńska, będących integralną częścią niniejszej Polityki:

1. Polityka bezpieczeństwa przetwarzania danych osobowych
2. Instrukcja zarządzania systemem informatycznym
3. Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych wraz z załącznikiem nr 1, nr 3
4. Rejestr incydentów bezpieczeństwa oraz działań korygujących i Zapobiegawczych – tzw. Rejestr naruszeń (Załącznik nr 2)
5. Polityka prywatności wraz z klauzulą informacyjną
6. Polityka plików cookies
7. Procedura weryfikacji Podmiotów przetwarzających dane osobowe oraz Formularz weryfikacji Podmiotu przetwarzającego dane osobowe
8. Umowa powierzenia przetwarzania danych osobowych - wzór
9. Wniosek o realizację praw osoby, której dane dotyczą zgodnie z Rozporządzeniem RODO
10. Metodologia oceny ryzyka wraz z analizą
11. Dokumentacja pracownicza zgodna z RODO

### **§2. Zakres przedmiotowy Polityki ochrony danych osobowych**

Polityka zawiera opis zasad ochrony danych osobowych obowiązujących w Przedsiębiorstwie: Midorino Judo Teresa Klaczyńska ul. Dębowa 39/2, 61-458 Poznań.

### **§3. Podmioty odpowiedzialne**

Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest Administrator danych osobowych.

### **§4. Skróty i definicje**

**Polityka** – oznacza niniejszy dokument, o ile co innego nie wynika wyraźnie z kontekstu.

**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.

**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, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

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

**Dane dzieci** – oznaczają dane osób poniżej 16 roku życia.

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

**Podmiot przetwarzający** – oznacza organizację lub osobę, której Przedsiębiorstwo powierzyło przetwarzanie danych osobowych (np. firma księgowa, prawnicza, usługodawca IT).

**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.

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

**IOD lub Inspektor** oznacza Inspektora Ochrony Danych Osobowych.

**Administrator danych osobowych lub Administrator** rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

**Przedsiębiorstwo** oznacza: Midorino Judo Teresa Klaczyńska ul. Dębowa 39/2 61-458 Poznań

## **§5. Zasady ogólne ochrony danych osobowych**

### **5.1. Filary ochrony danych osobowych**

**zasada legalności** – Administrator danych osobowych dba o ochronę prywatności i przetwarza dane zgodnie z prawem;

**zasada bezpieczeństwa** – Administrator danych osobowych zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stałe działania w tym zakresie;

**zasada rozliczalności** – Administrator danych osobowych dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność z prawem;

**prawa jednostki** – Administrator danych osobowych umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.

### **5.2. Zasady ochrony danych osobowych**

Administrator danych osobowych przetwarza dane osobowe z poszanowaniem następujących zasad.

w oparciu o podstawę prawną i zgodnie z prawem;

- a) rzetelnie i uczciwie;
- b) w sposób przejrzysty dla osoby, której dane dotyczą;
- c) w konkretnych celach;
- d) w niezbędnym zakresie;
- e) z dbałością o prawidłowość danych;
- f) nie dłużej niż potrzeba;
- g) zapewniając odpowiednie bezpieczeństwo.

### 5.3. System ochrony danych osobowych

**Inwentaryzacja danych:** Administrator danych osobowych dokonuje identyfikacji zasobów danych osobowych, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych, w tym: przypadków przetwarzania danych szczególnych kategorii i danych karnych, przypadków przetwarzania danych dzieci, profilowania, współadministrowania danymi;

**Podstawy prawne:** Administrator danych osobowych zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych.

**Obsługa praw jednostki:** Administrator danych osobowych spełnia obowiązki informacyjne względem osób, których dane przetwarza oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:

- a) obowiązki informacyjne. Administrator danych osobowych przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia dokumentowanie realizacji tych obowiązków;
- b) możliwość wykonywania żądań. Administrator danych osobowych weryfikuje i zapewnia możliwość efektywnego wykonywania każdego typu żądania przez siebie i swoich przetwarzających;
- c) obsługa żądań. Administrator danych osobowych zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany przez RODO i dokumentowane;
- d) zawiadamianie o naruszeniach. Administrator danych osobowych stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

5.4. **Bezpieczeństwo.** Administrator danych osobowych 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 jest wysokie;
- c) dostosowuje środki ochrony danych do ustalonego ryzyka;
- d) posiada system zarządzania bezpieczeństwem informacji;
- e) stosuje procedury pozwalające na identyfikację, ocenę i zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych – zarządzanie incydentami.

5.5. **Przetwarzający.** Administrator danych osobowych posiada zasady doboru przetwarzających dane na jego rzecz, wymogów co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia.

5.6. **Privacy by design.** Administrator danych osobowych zarządza zmianami wpływającymi na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji uwzględniają konieczność oceny wpływu zmiany na ochronę danych, analizę ryzyka, zapewnienie prywatności już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.

## §6. Żądania osób

1. **Dostęp do danych.** Na żądanie osoby dotyczącej dostępu do jej danych Administrator danych osobowych informuje osobę, czy przetwarza jej dane oraz informuje 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.

2. **Kopie danych.** Na żądanie Administrator danych osobowych wydaje kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Za kolejne kopie danych Administrator danych osobowych zastrzega prawo do pobierania opłat.

3. **Sprostowanie danych.** Administrator danych osobowych dokonuje sprostowania nieprawdziwych/nieprawidłowych danych na żądanie osoby. Administrator danych osobowych ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Administrator danych osobowych informuje osobę o odbiorcach danych, na żądanie tej osoby.

4. **Uzupełnienie danych.** Administrator danych osobowych uzupełnia i aktualizuje dane na żądanie osoby. Administrator danych osobowych ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych. Administrator danych osobowych może polegać na oświadczeniu osoby co do uzupełnienia danych, chyba że istnieją podstawy, aby uznać to oświadczenie za niewiarygodne.

5. **Usunięcie danych.** Na żądanie osoby Administrator danych osobowych usuwa dane, gdy:

- ☐ dane nie są niezbędne do celów, w których zostały zebrane, ani przetwarzane w innych zgodnych z prawem celach;
- ☐ zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania;
- ☐ osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych;
- ☐ dane były przetwarzane niezgodnie z prawem;
- ☐ konieczność usunięcia wynika z obowiązku prawnego;
- ☐ żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.

6. Administrator danych osobowych 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.

7. W przypadku, gdy dane podlegające usunięciu zostały upublicznione przez Przedsiębiorcę, Przedsiębiorca podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe o potrzebie usunięcia danych i dostępu do nich.

8. W przypadku usunięcia danych Administrator danych osobowych informuje osobę o odbiorcach danych, na żądanie tej osoby.

9. **Realizacja praw osób fizycznych w zakresie przetwarzania danych osobowych odbywa się na podstawie złożenia drogą elektroniczną, pocztową lub osobiście w siedzibie Administratora – Wniosku o realizację praw osoby, której dane dotyczą zgodnie z Rozporządzeniem RODO.**

## **§7. Ograniczenie przetwarzania**

1. Administrator danych osobowych dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:

- a) **osoba kwestionuje prawidłowość danych** – na okres pozwalający sprawdzić ich prawdziwość/prawidłowość;
- b) **przetwarzanie jest niezgodne z prawem**, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
- c) **Administrator danych osobowych nie potrzebuje już danych osobowych**, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
- d) **osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją** do czasu

stwierdzenia, czy po stronie Administrator danych osobowych zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

2. W trakcie ograniczenia przetwarzania Administrator danych osobowych 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.

3. W przypadku ograniczenia przetwarzania danych Administrator danych osobowych informuje osobę o odbiorcach danych, na żądanie tej osoby.

## **§8. Przenoszenie danych**

1. Na żądanie osoby Administrator danych osobowych 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 Administrator danych osobowych, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej w systemach informatycznych Administrator danych osobowych.

2. Sprzeciw w szczególnej sytuacji. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Administrator danych osobowych w oparciu o uzasadniony interes Administrator danych osobowych lub o powierzone Administrator danych osobowych w interesie publicznym, Administrator danych osobowych uwzględni sprzeciw, o ile nie zachodzą po stronie Administrator danych osobowych ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

3. **Sprzeciw względem marketingu bezpośredniego:** jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Administrator danych osobowych na potrzeby marketingu bezpośredniego, Administrator danych osobowych uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

## **§9. Minimalizacja**

**1. Administrator danych osobowych dba o minimalizację przetwarzania danych pod kątem adekwatności danych do celów, dostępu do danych, czasu przechowywania danych.**

2. Minimalizacja zakresu. Administrator danych osobowych zweryfikował zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO.

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

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

**5. Minimalizacja dostępu.**

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

5.2. Administrator danych osobowych dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających.

5.3. Administrator danych osobowych dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.

**6. Minimalizacja czasu.**

6.1 Administrator danych osobowych wdraża mechanizmy kontroli cyklu życia danych osobowych, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych.

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

## **§10. Bezpieczeństwo**

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

**2. Analiza ryzyka i adekwatności środków bezpieczeństwa.** Administrator danych osobowych przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:

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

b) Administrator danych osobowych kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.

c) Administrator danych osobowych przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Administrator danych osobowych 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.

3. Administrator danych osobowych ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, środki zapewniające ciągłość działania zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

### **4. Ocena skutków dla ochrony danych**

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

Administrator danych osobowych stosuje metodykę oceny skutków przyjętą w przedsiębiorstwie.

### **5. Środki bezpieczeństwa**

Administrator danych osobowych 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 przedsiębiorstwie.

### **6. Zgłaszanie naruszeń.**

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

**Szczegółowa procedura: Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych.**

## **§11. Przetwarzający**

Administrator danych osobowych posiada zasady doboru i weryfikacji przetwarzających dane na rzecz Administrator danych osobowych 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 działalności gospodarczej.

Administrator danych osobowych przyjęła minimalne wymagania co do umowy powierzenia przetwarzania danych.

Administrator danych osobowych rozlicza przetwarzających z wykorzystania pod przetwarzających, jak też z innych wymagań wynikających z Zasad powierzenia danych osobowych.

**Szczegółowa procedura: Procedura weryfikacji podmiotu przetwarzającego.**

## **§12. Eksport danych**

W przedsiębiorstwie nie dochodzi do eksportu danych, czyli przekazywania danych poza Europejski Obszar Gospodarczy.

## **§13. Projektowanie prywatności**

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

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

**Niniejsza Polityka Ochrony Danych Osobowych wchodzi w życie z dniem \_\_\_\_\_ r.**

|                             |
|-----------------------------|
| Zatwierdził w dniu _____ r. |
|                             |