# POLITYKA PRYWATNOŚCI

## I. POSTANOWIENIA OGÓLNE

Polityka prywatności (dalej: **Polityka**) stanowi opis wymogów, zasad i regulacji ochrony danych osobowych w ramach współadministrowania danymi osobowymi przez podmioty z Grupy ECDP.

Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu art. 24 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. RODO - 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) (dalej: **RODO**).

Polityka zawiera:

1. opis zasad ochrony danych osobowych obowiązujących w Grupie ECDP.
2. odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach).

Odpowiedzialny za:

1. wdrożenie i utrzymanie niniejszej Polityki jest Zarząd każdej ze spółek wchodzących w skład w Grupy ECDP.
2. nadzór i monitorowanie przestrzegania Polityki - Zarząd każdej ze spółek wchodzących w skład w Grupy ECDP.
3. stosowanie do niniejszej Polityki – wszyscy członkowie personelu i współpracownicy każdej ze spółek wchodzących w skład w Grupy ECDP.

## II. SKRÓTY I DEFINICJE

| | |
|---|---|
| **Polityka** | oznacza niniejszą Politykę prywatności, o ile co innego nie wynika wyraźnie z kontekstu; |
| **Administrator danych** | ECDP TAX Spółka z ograniczoną odpowiedzialnością, ul. Plac Wolności 4, 40-078 Katowice, KRS: 0000754504; |
| **RODO** | oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. RODO - 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); |
| **Dane** | oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu; |
| **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; |
| **Osoba** | oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu; |
| **Podmiot przetwarzający** | oznacza organizację lub osobę, której Spółka powierzyła przetwarzanie danych osobowych (np. usługodawca IT, pomioty zajmujące się windykacją należności); |
| **Profilowanie** | oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które podlega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy i 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; |
| **RCPD** | oznacza Rejestr Czynności Przetwarzania Danych Osobowych; |
| **RKCPD** | oznacza Rejestr Kategorii Czynności Przetwarzania Danych. |

## III. ZASADY OCHRONY DANYCH OSOBOWYCH

Podmioty z Grupy ECDP przetwarzają dane osobowe z uwzględnieniem:

1. **Legalności –** dbałość o ochronę prywatności i przetwarzanie danych zgodnie z prawem,

2. **Bezpieczeństwa –** zapewnienie odpowiedniego poziomu bezpieczeństwa danych, poprzez podejmowanie stałych działań w tym zakresie,
3. **Praw jednostki –** umożliwienie osobom, których dane przetwarza, wykonywanie i realizację swoich praw i prawa te realizuje,
4. **Rozliczalności** – dokumentowanie to, w jaki sposób spełnia swoje obowiązki, aby w każdej chwili móc wykazać zgodność.

Podmioty z Grupy ECDP przetwarzają 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).***

## IV. SYSTEM OCHRONY DANYCH OSOBOWYCH

System ochrony danych osobowych w Podmiotach z Grupy ECDP obejmuje następujące obszary:

### 1. Inwentaryzacja danych

Podmioty z Grupy ECDP dokonują identyfikacji zasobów danych osobowych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych (inwentaryzacja).

### 2. Rejestrowanie czynności przetwarzania

Podmioty z Grupy ECDP prowadzą i utrzymuje Rejestr Czynności Przetwarzania Danych (RCPD) oraz Rejestr Kategorii Czynności Przetwarzania Danych (RKCPD).

**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 danych, czyli zasady rozliczalności.

**RCPD** jest jednym z podstawowych narzędzi umożliwiających rozliczanie większości obowiązków ochrony danych.

Przetwarzanie jest zgodne z prawem w przypadkach, gdy spełniony jest co najmniej jeden z poniższych warunków:

a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze danych;
d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych w szczególności, gdy osoba, której dane dotyczą, jest dzieckiem.

## 3. Obsługa praw jednostki

Podmioty z Grupy ECDP wykonują obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:

a) obowiązki informacyjne – podmioty z Grupy ECDP przekazują przy zbieraniu danych i w innych sytuacjach określonych prawem, wymagane informacje oraz organizuje i zapewnia udokumentowanie realizacji obowiązków w tym zakresie;
b) możliwość wykonania żądań – podmioty z Grupy ECDP weryfikują i zapewniają możliwość efektywnego wykonania każdego typu żądania kierowanego do Administratora danych;
c) obsługa żądań – podmioty z Grupy ECDP zapewniają odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany przez RODO i dokumentowane;
d) zawiadamianie o naruszeniach - podmioty z Grupy ECDP stosują procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

Podmioty z Grupy ECDP podejmują odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14 RODO oraz prowadzić z nią wszelką

komunikację na mocy art. 15–22 i 34 RODO w sprawie przetwarzania. Informacji udziela się na piśmie lub elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą. Podmioty z Grupy ECDP wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.

Podmioty z Grupy ECDP bez zbędnej zwłoki zawiadamia osobę o naruszeniu danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

Podmioty z Grupy ECDP dokumentują obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

## 4. Żądania osób

Realizując prawa osób, których dane dotyczą, podmioty z Grupy ECDP wprowadzają 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), Administrator danych może się zwrócić do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

Czynności podejmowane przez Administratora danych w związku z żądaniami osób:

a) **Nieprzetwarzanie –** Administrator danych informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw,
b) **Odmowa –** Administrator danych informuje osobę, w ciągu miesiąca od otrzymania żądania
o odmowie rozpatrzenia żądania podając jednocześnie podstawę prawną takiej odmowy i o prawach osoby z tym związanych,
c) **Dostęp do danych -** Na żądanie osoby dotyczące dostępu do jej danych Administrator danych 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 w postaci wydruku bądź w formie elektronicznej w czytelnym maszynowo formacie z zastrzeżeniem, że kopii danych wydanej w wykonywaniu prawa dostępu do danych Administrator danych nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych,

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

e) **Sprostowanie danych –** Administrator danych 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,

f) **Uzupełnienie danych –** Administrator danych uzupełnia i aktualizuje dane na żądanie osoby. Administrator danych ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych. Administrator danych może polegać na oświadczeniu osoby co do uzupełnienia danych, chyba że będzie to nie wystarczające w świetle procedur, prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne,

g) **Usunięcie danych -** Na żądanie osoby Administrator danych 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,

Podmioty z Grupy ECDP określają 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 podmioty z Grupy ECDP, podmiot ten podejmie rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe o potrzebie usunięcia danych i dostępu do nich,

h) **Ograniczenie przetwarzania –** Spółka dokonuje ograniczenia przetwarzania danych na żądanie osoby. W trakcie ograniczenia przetwarzania Spółka 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. Spółka informuje osobę przed uchyleniem ograniczenia przetwarzania. W przypadku ograniczenia przetwarzania danych Spółka informuje osobę o odbiorcach danych, na żądanie tej osoby.

i) **Przenoszenie danych –** Na żądanie osoby Spółka 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 Spółka, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Spółka,

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

k) **Sprzeciw względem marketingu bezpośredniego.** Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Spółka na potrzeby marketingu bezpośredniego (w tym ewentualnie profilowania), Spółka uwzględni sprzeciw i zaprzestanie takiego przetwarzania,

## 5. Minimalizacja

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

a) **zasady zarządzania adekwatnością danych** – Podmioty weryfikują zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO. Podmiotu dokonują przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok. Podmioty przeprowadzają weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (*privacy by design),*

b) **zasady reglamentacji i zarządzania dostępem do danych** – Podmioty stosują 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). Podmioty stosują kontrolę dostępu fizycznego. Podmioty dokonują aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób oraz zmianach podmiotów przetwarzających.

c) **zasady zarządzania okrese**m **przechowywania danych i weryfikacji dalszej przydatności** – Podmioty wdrażają mechanizmy kontroli cyklu życia danych osobowych, 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 informatycznych Spółki,

jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Podmioty

## 6. Bezpieczeństwo

Podmioty z Grupy ECDP zapewniają odpowiedni poziom bezpieczeństwa danych, w tym:

a) przeprowadzają analizy ryzyka dla czynności przetwarzania danych lub ich kategorii,
b) przeprowadzają oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie,
c) dostosowują środki ochrony danych do ustalonego ryzyka,
d) stosują procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych **Prezesowi Urzędu Ochrony Danych Osobowych** (zarządza incydentami).

Podmioty zapewniają stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych.

### 6.1. Analiza ryzyka i adekwatności środków bezpieczeństwa

Podmioty z Grupy ECDP przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:

a) zapewniają odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania - wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych,
b) kategoryzują dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają,
c) przeprowadzają analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii, w oparciu o przyjętą metodykę. Administrator danych 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) ustalają możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrożenia,
e) ustalają przydatność i stosuje takie środki i podejście, jak:
    - pseudonimizacja,
    - anonimizacja
    - szyfrowanie danych osobowych,
    - inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności systemów informatycznych i usług przetwarzania,

- 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.

6.2. Ocena skutków dla ochrony danych

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.

6.3. Środki bezpieczeństwa

Podmioty stosują środki bezpieczeństwa ustalone w ramach analizy ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych. Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa.

**6.4. Zgłaszanie naruszeń**

Podmioty stosują procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych **Prezesowi Urzędu Ochrony Danych Osobowych** w terminie 72 godzin od ustalenia naruszenia.

## 8. Powierzenie przetwarzania danych osobowych

Podmioty posiadają i stosują zasady doboru i weryfikacji podmiotów przetwarzających dane na ich rzecz, 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 Podmiotach.

## 9. Zarządzanie zmianą (*privacy by design*)

Podmioty zarządzają 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 Podmioty odwołują się do zasad bezpieczeństwa danych osobowych, a także uwzględniają konieczność oceny wpływu zmiany na ochronę danych, analizę ryzyka, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.

# V. POSTANOWIENIA KOŃCOWE

W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy RODO oraz UODO.