POLITYKA PRYWATNOŚCI

Polityka ochrony danych osobowych

Administrator: Karolina Plis prowadzący działalność gospodarczą pod firmą: Karolina Plis Finanse i Nieruchomości, ul. Mazowiecka 44, 74-100 Gryfino, NIP: 8581791880, REGON 529723039 oraz Anna Maziarz prowadząca działalność gospodarczą pod firmą: Anna Maziarz, ul. Jana Pawła II 44AA/1,74-100 Gryfino, NIP: 8581677138, REGON 541754556.

1. Cel i podstawa dokumentu

Dokument „Polityka ochrony danych osobowych" (dalej: Polityka) stanowi mapę wymogów, zasad i regulacji ochrony danych osobowych w ATELIER NIERUCHOMOŚCI

Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO — rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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) (Dz. Urz. UE L 2016 nr 119, s. 1).

Polityka zawiera:

opis zasad ochrony danych obowiązujących w Przedsiębiorstwie,
odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące obszarów wymagających doprecyzowania w odrębnych dokumentach).

Odpowiedzialny za wdrożenie, utrzymanie i stosowanie niniejszej Polityki jest Przedsiębiorca.
2. Definicje

Polityka — polityka ochrony danych osobowych, o ile co innego nie wynika z kontekstu.
RODO — rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r.
Dane — dane osobowe, o ile co innego nie wynika z kontekstu.
Dane szczególnej kategorii — dane z art. 9 ust. 1 RODO, m.in. dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne i biometryczne (w celu jednoznacznej identyfikacji), dane dotyczące zdrowia, seksualności lub orientacji seksualnej.
Dane karne — dane z art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa.
Dane dzieci — dane osób poniżej 16. roku życia.
Osoba — osoba, której dane dotyczą.
Podmiot przetwarzający — organizacja lub osoba, której Przedsiębiorca powierzył przetwarzanie danych (np. usługodawca IT, zewnętrzna księgowość).
Profilowanie — zautomatyzowane przetwarzanie danych osobowych służące ocenie czynników osobowych osoby fizycznej (np. analiza efektywności pracy, sytuacji ekonomicznej, zdrowia, preferencji, zachowania, lokalizacji).

Eksport danych — przekazanie danych do państwa trzeciego lub organizacji międzynarodowych.

IOD / Inspektor — Inspektor Ochrony Danych Osobowych.

RCPD / Rejestr — Rejestr Czynności Przetwarzania Danych Osobowych.

Przedsiębiorca — osoba fizyczna: Krzysztof Makowski, prowadzący działalność gospodarczą pod firmą ELITE NIERUCHOMOŚCI KRZYSZTOF MAKOWSKI, z/s w Szczecinie, ul. S. I. Witkiewicza 58 lok. U-19, 71-125 Szczecin, NIP 955-194-58-47.

3. Ochrona danych osobowych w Przedsiębiorstwie — zasady ogólne 3.1. Filary ochrony danych

Legalność — przetwarzanie danych zgodnie z prawem i z poszanowaniem prywatności.

Bezpieczeństwo — zapewnienie adekwatnego poziomu bezpieczeństwa danych i stałe doskonalenie zabezpieczeń.

Prawa jednostki — umożliwienie i realizacja praw osób, których dane są przetwarzane.

Rozliczalność — dokumentowanie sposobów spełniania obowiązków i zdolność wykazania zgodności w każdym czasie.

3.2. Zasady przetwarzania danych

Przedsiębiorca przetwarza dane osobowe z poszanowaniem zasad:

legalizmu — w oparciu o podstawę prawną i zgodnie z prawem;
rzetelności — rzetelnie i uczciwie;
transparentności — w sposób przejrzysty dla osoby;
celowości i minimalizacji — w konkretnych celach i nie „na zapas”;
adekwatności — nie więcej niż potrzeba;
prawidłowości — z dbałością o poprawność danych;
czasowości — nie dłużej niż potrzeba;
bezpieczeństwa — z zapewnieniem odpowiednich środków ochrony.

3.3. System ochrony danych — elementy

I. Inwentaryzacja danych. Identyfikacja zasobów danych, klas danych, zależności między zasobami oraz sposobów ich wykorzystania, w tym:

przypadków przetwarzania danych szczególnych kategorii i danych karnych,
przetwarzania danych osób niezidentyfikowanych (UFO),
przetwarzania danych dzieci,
profilowania,
współadministrowania danymi.

II. Rejestr (RCPD). Opracowanie, prowadzenie i utrzymanie Rejestru Czynności Przetwarzania Danych jako narzędzia rozliczania zgodności.

III. Podstawy prawne. Zapewnienie, identyfikacja i weryfikacja podstaw prawnych przetwarzania oraz ich rejestracja w RCPD, w tym:

system zarządzania zgodami na przetwarzanie i komunikację na odległość,
inwentaryzacja i uszczegółowienie uzasadnienia przetwarzania na podstawie prawnie uzasadnionego interesu.

IV. Umowy powierzenia. Zawieranie umów powierzenia przetwarzania danych z podmiotami przetwarzającymi (art. 28 RODO).

V. Obsługa praw jednostki.

obowiązki informacyjne i ich udokumentowanie,
weryfikacja i zapewnienie możliwości wykonania żądań,
terminowa realizacja żądań i ich dokumentowanie,
zawiadamianie o naruszeniach.

VI. Minimalizacja (privacy by default).

zarządzanie adekwatnością danych,
reglamentacja i zarządzanie dostępem,
zarządzanie okresem przechowywania i weryfikacją przydatności.

VII. Bezpieczeństwo.

analizy ryzyka i oceny skutków (DPIA),
dostosowanie środków ochrony do ryzyka,
system zarządzania bezpieczeństwem informacji (w tym systemem informatycznym),
procedury identyfikacji, oceny i zgłaszania naruszeń (zarządzanie incydentami).

VIII. Privacy by design. Zarządzanie zmianami z uwzględnieniem ochrony danych już na etapie projektowania.

IX. Przetwarzający. Zasady doboru przetwarzających, warunków powierzenia oraz weryfikacji wykonania umów powierzenia.

X. Eksport danych. Weryfikacja przekazywania danych poza UE/EOG lub do organizacji międzynarodowych i zapewnienie zgodnych z prawem warunków przekazania.

XI. Przetwarzanie transgraniczne. Ustalenie przypadków przetwarzania transgranicznego oraz wiodącego organu nadzorczego i głównej jednostki organizacyjnej.

4. Rejestr Czynności Przetwarzania Danych (RCPD)

Cel RCPD. RCPD dokumentuje czynności przetwarzania i pełni rolę mapy przetwarzania danych, umożliwiając realizację zasady rozliczalności.

Prowadzenie. Przedsiębiorstwo prowadzi RCPD, inwentaryzując i monitorując sposoby wykorzystania danych osobowych.

Narzędzie rozliczalności. RCPD umożliwia rozliczanie większości obowiązków ochrony danych.

Zakres wpisów. Dla każdej czynności odnotowuje się co najmniej:

(a) nazwę czynności,
(b) cel przetwarzania,
(c) opis kategorii osób,
(d) opis kategorii danych,
(e) podstawę prawną (w tym kategorie uzasadnionego interesu),
(f) sposób zbierania danych,
(g) kategorie odbiorców (w tym przetwarzających),
(h) informacje o przekazaniu poza UE/EOG,
(i) ogólny opis środków technicznych i organizacyjnych ochrony.

Wzór RCPD stanowi Załącznik nr 1 do Polityki („Wzór Rejestru Czynności Przetwarzania Danych") i zawiera również kolumny nieobowiązkowe, które mogą być uzupełniane w miarę potrzeb.

5. Podstawy przetwarzania

Przedsiębiorstwo dokumentuje w RCPD podstawy prawne przetwarzania danych dla poszczególnych czynności.

Wskazując ogólną podstawę (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony interes), Przedsiębiorstwo doprecyzowuje ją w razie potrzeby (np. konkretny przepis, zakres zgody, kategorie zdarzeń).

Wdrożone są metody zarządzania zgodami, w tym rejestracja udzielonych zgód, odmów, cofnięć i sprzeciwów (także dot. komunikacji na odległość: e-mail, telefon, SMS itp.).

Przedsiębiorca zna podstawy prawne każdej czynności przetwarzania oraz — w przypadku uzasadnionego interesu — jego konkretny cel (np. marketing własny, dochodzenie roszczeń).

6. Sposób obsługi praw jednostki i obowiązków informacyjnych

Przedsiębiorstwo dba o czytelność i styl komunikacji z osobami, których dane przetwarza.

Ułatwia korzystanie z praw poprzez m.in. publikację informacji na stronie internetowej (w tym wymogi identyfikacji, metody kontaktu, ewentualny cennik żądań dodatkowych).

Dotrzymuje prawnych terminów realizacji obowiązków względem osób.

Zapewnia procedury identyfikacji, integracji, modyfikacji i usuwania danych konkretnych osób w sposób zintegrowany.

Dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

7. Obowiązki informacyjne

Określenie zgodnych z prawem i efektywnych sposobów wykonywania obowiązków informacyjnych.

Informowanie osoby o przedłużeniu ponad jeden miesiąc terminu rozpatrzenia żądania.

Informowanie przy pozyskiwaniu danych bezpośrednio od osoby.

Informowanie przy pozyskiwaniu danych pośrednio (od innego podmiotu).

Określenie sposobu informowania o przetwarzaniu danych niezidentyfikowanych (np. monitoring wizyjny).

Informowanie o planowanej zmianie celu przetwarzania.

Informowanie przed uchyleniem ograniczenia przetwarzania.

Informowanie odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu (chyba że wymagałoby to niewspółmiernie dużego wysiłku lub byłoby niemożliwe).

Informowanie o prawie sprzeciwu najpóźniej przy pierwszym kontakcie.

Niezwłoczne zawiadamianie osoby o naruszeniu, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności.

8. Żądania osób

8.1. Nieprzetwarzanie

Informowanie osoby, że jej dane nie są przetwarzane — jeżeli zgłosiła żądanie dotyczące jej praw.

8.2. Odmowa

Informowanie osoby w ciągu miesiąca o odmowie rozpatrzenia żądania oraz o przysługujących jej prawach.

8.3. Dostęp do danych

Na żądanie — informacja, czy dane są przetwarzane, wraz ze szczegółami (art. 15 RODO) oraz dostęp do danych (np. poprzez kopię danych; wydanie kopii w ramach prawa dostępu nie stanowi „pierwszej bezpłatnej kopii”
dla celów opłat).

8.4. Kopie danych

Wydanie kopii danych na żądanie oraz odnotowanie wydania pierwszej kopii.

8.5. Sprostowanie danych

Sprostowanie danych na żądanie osoby; możliwa odmowa, jeśli brak wykazania nieprawidłowości. Informowanie o odbiorcach — na żądanie osoby.

8.6. Uzupełnienie danych

Uzupełnianie i aktualizacja na żądanie, z prawem odmowy, jeżeli byłoby to niezgodne z celami przetwarzania. Co do zasady — możliwość oparcia się na oświadczeniu osoby, o ile jest wystarczające i wiarygodne.

8.7. Usunięcie danych

Usunięcie danych na żądanie, gdy:

dane nie są niezbędne do celów, dla których zostały zebrane lub przetwarzane;
zgoda została cofnięta, a brak innej podstawy prawnej;
osoba wniosła skuteczny sprzeciw;
dane były przetwarzane niezgodnie z prawem;
obowiązek usunięcia wynika z prawa.

Przedsiębiorstwo zapewnia efektywną realizację prawa do usunięcia, z poszanowaniem zasad ochrony danych i wyjątków z art. 17 ust. 3 RODO.
Jeżeli dane zostały upublicznione, podejmowane są rozsądne działania (w tym techniczne) w celu poinformowania innych administratorów o potrzebie usunięcia danych i dostępu do nich. Informowanie o odbiorcach — na żądanie osoby.

8.8. Ograniczenie przetwarzania

Ograniczenie przetwarzania na żądanie osoby, gdy:

a) kwestionuje prawidłowość danych — na czas weryfikacji,
b) przetwarzanie jest niezgodne z prawem, a osoba sprzeciwia się usunięciu,
c) dane nie są potrzebne Przedsiębiorstwu, lecz są potrzebne osobie do ustalenia, dochodzenia lub obrony roszczeń,
d) wniesiono sprzeciw z przyczyn związanych ze szczególną sytuacją — do czasu stwierdzenia, czy po stronie Przedsiębiorstwa zachodzą nadrzędne podstawy.

W okresie ograniczenia — przechowywanie bez przetwarzania (z wyjątkami: roszczenia, ochrona praw innych osób, ważny interes publiczny).
Informowanie osoby przed uchyleniem ograniczenia oraz — na żądanie — o odbiorcach danych.

9. Minimalizacja

Przedsiębiorstwo dba o minimalizację przetwarzania danych w zakresie:

adekwatności (ilości danych i zakresu przetwarzania),
dostępu do danych,
czasu przechowywania danych.

9.1. Minimalizacja zakresu

Weryfikacja zakresu pozyskiwania i przetwarzania danych w ramach wdrożenia RODO.
Okresowy przegląd ilości i zakresu przetwarzania — nie rzadziej niż raz w roku.
Weryfikacja zmian w procedurach zarządzania zmianą (privacy by design).

9.2. Minimalizacja dostępu

Ograniczenia dostępu: prawne (zobowiązania poufności, upoważnienia), fizyczne (strefy dostępu, zamykanie pomieszczeń), logiczne (uprawnienia w systemach i zasobach sieciowych).
Kontrola dostępu fizycznego.
Aktualizacje uprawnień przy zmianach personelu/ról oraz podmiotów przetwarzających.
Okresowy przegląd użytkowników systemów — nie rzadziej niż raz w roku.
Szczegóły w procedurach bezpieczeństwa fizycznego i informacji.

9.3. Minimalizacja czasu

Mechanizmy kontroli cyklu życia danych (weryfikacja przydatności vs. terminy i punkty kontrolne w RCPD).

Usuwanie danych z systemów produkcyjnych oraz z akt po upływie przydatności; dane mogą pozostawać w archiwach i kopiach zapasowych zgodnie z procedurami.

10. Zgłaszanie naruszeń ochrony danych organowi nadzorczemu

Termin zgłoszenia. W razie naruszenia ochrony danych Przedsiębiorca bez zbędnej zwłoki — w miarę możliwości nie później niż 72 godziny od stwierdzenia naruszenia — zgłasza je właściwemu organowi nadzorczemu (art. 55 RODO), chyba że jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Zgłoszenia po 72 godzinach zawierają wyjaśnienie przyczyn opóźnienia.

Zakres zgłoszenia. Zgłoszenie obejmuje co najmniej:

a) opis charakteru naruszenia, w tym — w miarę możliwości — kategorie i przybliżoną liczbę osób oraz wpisów danych, których dotyczy naruszenie,

b) dane kontaktowe IOD lub innego punktu kontaktowego,

c) opis możliwych konsekwencji naruszenia,

d) opis zastosowanych lub proponowanych środków zaradczych (w tym minimalizujących skutki).

Dokumentowanie. Przedsiębiorca dokumentuje wszelkie naruszenia, ich okoliczności, skutki oraz podjęte działania zaradcze.

11. Postanowienia końcowe

W zakresie nieuregulowanym niniejszą Polityką zastosowanie mają przepisy z zakresu ochrony danych osobowych.

O wszelkich zmianach Polityki Przedsiębiorca powiadomi drogą mailową lub listowną.

Niniejsza Polityka obowiązuje od 01.06.2025 r.