POLITYKA BEZPIECZEŃSTWA INFORMACJI

6 CZERWCA 2023

KANCELARIA PRAWNICZA JAN IKSIŃSKI

I. Postanowienia ogólne

1. Polityka dotyczy wszystkich Danych osobowych przetwarzanych w Kancelarii Prawniczej Jan Iksiński, niezależnie od formy ich przetwarzania (przetwarzane tradycyjnie zbiory ewidencyjne, systemy informatyczne) oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych.

2. Polityka jest przechowywana w wersji elektronicznej oraz w wersji papierowej w siedzibie Administratora.

3. Polityka jest udostępniana do wglądu osobom posiadającym upoważnienie do przetwarzania danych osobowych na ich wniosek, a także osobom, którym ma zostać nadane upoważnienie do przetwarzania danych osobowych, celem zapoznania się z jej treścią.

4. Zgodnie z art. 6 ustawy z 26 maja 1982 r. Prawo o Adwokaturze Dane osobowe przetwarzane w Kancelarii Prawniczej Jan Iksiński, a uzyskane w związku z udzielaniem pomocy prawnej przez adwokata, objęte są tajemnicą adwokacką. Adwokata nie można zwolnić od obowiązku zachowania tajemnicy zawodowej co do faktów, o których dowiedział się udzielając pomocy prawnej lub prowadząc sprawę.

5. W zakresie przetwarzania danych pozyskanych w związku z wykonywaniem czynności objętych tajemnicą adwokacką Administrator stosuje się do wskazanych powyżej przepisów dotyczących zachowania tajemnicy zawodowej.

6. Dla skutecznej realizacji Polityki Administrator Danych zapewnia:

a) odpowiednie do zagrożeń i kategorii danych objętych ochroną środki techniczne i rozwiązania organizacyjne,

b) kontrolę i nadzór nad Przetwarzaniem danych osobowych,

c) monitorowanie zastosowanych środków ochrony.

7. Monitorowanie przez Administratora Danych zastosowanych środków ochrony obejmuje m.in. działania Użytkowników, naruszanie zasad dostępu do danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.

8. Administrator Danych zapewnia, że czynności wykonywane w związku z przetwarzaniem i zabezpieczeniem danych osobowych są zgodne z niniejszą polityką oraz odpowiednimi przepisami prawa.

II. Dane osobowe przetwarzane u administratora danych

Za dane osobowe w rozumieniu art. 6 Ustawy uznaje się wszelkie informacje, dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Zatem, o ile dany zestaw informacji będzie umożliwiał bezpośrednią, bądź pośrednią identyfikację danej osoby, powinien być traktowany jako zawierający dane osobowe. O tym, czy dana informacja przejawia charakter osobowy przesądza zatem nie przynależność tej informacji do odpowiedniej kategorii, tylko kontekst, w jakim jest ona wykorzystywana oraz czy pozwala na zidentyfikowanie osoby.

III. Źródła danych

Administrator pozyskuje dane osobowe z poniższych źródeł:

- Klienci: dane osobowe pobierane są od klientów, w celu świadczenia im usług prawnych.
- Strony internetowe: Kancelaria Prawnicza Jan Iksiński prowadzi stronę internetową, na której może pozyskiwać dane osobowe, takie jak adresy e-mail czy numer telefonu, za pośrednictwem formularzy kontaktowych.

- Rejestr KRS: Kancelaria Prawnicza jest zobowiązana do wpisu do Krajowego Rejestru Sądowego (KRS), co oznacza, że jej dane, takie jak nazwa, adres i numer identyfikacji podatkowej, są publicznie dostępne.
- Bazy danych: Administrator może korzystać z baz danych, takich jak Rejestr Dłużników ERIF BIG czy Krajowy Rejestr Długów, w celu pozyskania informacji na temat swoich klientów lub przeciwników w sprawach sądowych.
- Social media: możliwe jest korzystanie z mediów społecznościowych, takich jak Facebook czy LinkedIn, w celu pozyskiwania danych osobowych potencjalnych klientów czy kontaktów biznesowych.

W każdym przypadku, Kancelaria Prawnicza musi przestrzegać przepisów dotyczących ochrony danych osobowych, takich jak RODO oraz dbać o poufność informacji pozyskanych od swoich klientów i innych osób.

Dokumenty: Dane osobowe przetwarzane zostają w wielu różnych dokumentach, w zależności od charakteru swojej działalności. Niektóre z najczęstszych dokumentów, w których przetwarzane są dane osobowe, to:

- Umowy: często przetwarza się dane osobowe swoich klientów w umowach, np. umowach o świadczenie usług prawnych czy umowach o pracę.
- Formularze: wykorzystuje się formularze, takie jak formularze kontaktowe na swoich stronach internetowych, aby zbierać dane osobowe klientów i potencjalnych klientów.
- Protokoły: tworzy si protokoły z przebiegu spotkań z klientami, które mogą zawierać dane osobowe.
- Dokumenty sądowe: tworzy się różnego rodzaju dokumenty procesowe, takie jak pozwania, odpowiedzi na pozwy czy wnioski procesowe, które zawierają dane osobowe stron.
- Korespondencja: Kancelarie prawnicze wymieniają się korespondencją, która również może zawierać dane osobowe.

Wszystkie dokumenty, w których przetwarzane są dane osobowe przez Administratora, muszą być zgodne z przepisami dotyczącymi ochrony danych osobowych, w tym RODO. Administrator jest również zobowiązany do dbania o poufność informacji pozyskanych od swoich klientów i innych osób.

Obszar przetwarzania to: archiwum, w którym znajdują się dane oraz komputer służbowy, dyski twarde zewnętrznych serwerów hostingowych, a także papierowe dokumenty (umowy, formularze).

IV. Obowiązki i odpowiedzialność w zakresie zarządzania bezpieczeństwem

Obowiązki

4.1. Zarządzanie bezpieczeństwem

4.1.1. Zarząd Kancelarii Prawniczej Jan Iksiński jest odpowiedzialny za ustanowienie i utrzymanie polityki bezpieczeństwa, która obejmuje zarządzanie ryzykiem, ochronę danych i zasobów, a także planowanie kontynuacji działalności.

4.1.2. Każdy pracownik Kancelarii Prawniczej Jan Iksiński ma obowiązek przestrzegania polityki bezpieczeństwa, procedur i wytycznych związanych z bezpieczeństwem.

4.1.3. Osoba odpowiedzialna za zarządzanie bezpieczeństwem (Security Manager) jest upoważniona do monitorowania, analizowania i zapewniania skutecznego funkcjonowania systemów bezpieczeństwa, w tym śledzenia incydentów i reagowania na nie.

4.2. Zarządzanie dostępem

4.2.1. Zarząd Kancelarii Prawniczej Jan Iksiński jest odpowiedzialny za zarządzanie dostępem do systemów, aplikacji i danych, określając uprawnienia i zabezpieczając je przed nieuprawnionym dostępem.

4.2.2. Każdy pracownik jest odpowiedzialny za zachowanie poufności swoich danych logowania, nieudostępnianie ich innym osobom i korzystanie z nich wyłącznie do celów służbowych.

4.3. Zarządzanie ryzykiem

4.3.1. Zarząd Kancelarii Prawniczej XYZ jest odpowiedzialny za identyfikację, ocenę i zarządzanie ryzykiem związanym z bezpieczeństwem informacji, w tym wdrażanie odpowiednich środków kontrolnych.

4.3.2. Każdy pracownik jest zobowiązany do zgłaszania wszelkich potencjalnych zagrożeń lub incydentów bezpieczeństwa do osoby odpowiedzialnej za zarządzanie bezpieczeństwem.

Odpowiedzialność

4.4.1 Zarząd Kancelarii Prawniczej Jak Iksiński ponosi ostateczną odpowiedzialność za skuteczne zarządzanie bezpieczeństwem, w tym ochronę danych i zasobów firmy.

4.4.2 Każdy pracownik jest odpowiedzialny za przestrzeganie polityki bezpieczeństwa, procedur i wytycznych związanych z bezpieczeństwem, a także za zgłaszanie wszelkich zagrożeń lub naruszeń bezpieczeństwa.

4.4.3 Osoba odpowiedzialna za zarządzanie bezpieczeństwem jest odpowiedzialna za monitorowanie i egzekwowanie przestrzegania polityki bezpieczeństwa, w tym podejmowanie odpowiednich działań w przypadku naruszeń lub incydentów bezpieczeństwa.

Niniejsza polityka bezpieczeństwa jest obowiązująca dla wszystkich pracowników Kancelarii Prawniczej Jan Iksiński i jest regularnie przeglądana i aktualizowana, aby odzwierciedlać zmieniające się wymogi i zagrożenia związane z bezpieczeństwem informacji."

V. Zarządzanie bezpieczeństwem informacji

5.1 Przetwarzanie danych osobowych:

Wszystkie osoby zobowiązane są do przetwarzania danych osobowych zgodnie z obowiązującymi przepisami oraz ustaloną Polityką Bezpieczeństwa, Instrukcją Zarządzania Systemem Informatycznym i innymi wewnętrznymi dokumentami i procedurami dotyczącymi przetwarzania danych osobowych w naszej kancelarii.

5.2 Zasady przetwarzania danych:

Wszystkie dane osobowe są przetwarzane zgodnie z zasadami przewidzianymi przez przepisy prawa. Obejmują one, między innymi, wyznaczenie prawnie uzasadnionych celów przetwarzania, minimalizację zakresu przetwarzanych danych, zapewnienie ich prawidłowości i aktualizacji, określenie okresu przechowywania danych oraz zapewnienie odpowiednich środków bezpieczeństwa.

5.3 Obowiązki Administratora Danych Osobowych:

Administrator Danych Osobowych ma szereg obowiązków związanych z organizacją bezpieczeństwa i ochroną danych osobowych. Obejmują one m.in. zapewnienie zgodności z Polityką Bezpieczeństwa, wydawanie i anulowanie upoważnień do przetwarzania danych, prowadzenie szkoleń dla użytkowników, kontrolę zgodności przetwarzania danych z przepisami o ochronie danych osobowych, nadzór nad bezpieczeństwem danych oraz zarządzanie incydentami i ochroną przed zagrożeniami.

5.4 Obowiązki osób upoważnionych do przetwarzania danych:

Osoby upoważnione do przetwarzania danych mają obowiązek znać i stosować środki ochrony danych osobowych oraz uniemożliwiać dostęp nieupoważnionym osobom. Przetwarzają one dane zgodnie z przepisami prawa i wewnętrznymi regulacjami, zachowują poufność danych, chronią dane i środki przetwarzające przed nieuprawnionym dostępem oraz informują Administratora Danych Osobowych o wszelkich podejrzeniach lub naruszeniach związanych z ochroną danych.