Kotarska
LAW & TAX

POLITYKA PRYWATNOŚCI
(Polityka ochrony danych osobowych)

1. Niniejszy dokument zatytułowany „**„Polityka Prywatności”** lub „**Polityka ochrony danych osobowych**” (dalej jako **Polityka**) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w **KANCELARII RADCY PRAWNEGO JOANNA KOTARSKA z siedzibą w Ustroniu przy ul. 9 Listopada 20** (dalej jako **Kancelaria)**. Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 119, s. 1).

2. Polityka zawiera:

   a) opis zasad ochrony danych obowiązujących w Kancelarii;

   b) odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach);

3. Odpowiedzialna za wdrożenie i utrzymanie niniejszej Polityki jest Joanna Kotarska, której powierzono nadzór nad obszarem ochrony danych osobowych oraz zapewnienie zgodności z ochroną danych osobowych; za stosowanie niniejszej Polityki odpowiedzialni są:

(i) wszyscy członkowie personelu Kancelarii.

Kancelaria powinna też zapewnić zgodność postępowania kontrahentów Kancelarii z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez Kancelarię.

4. **Skróty i definicje:**

Polityka oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu.
RODO oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 119, s. 1).
Dane oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu.
Dane wrażliwe oznaczają dane specjalne i dane karne.
Dane specjalne 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 Kancelaria powierzyła przetwarzanie danych osobowych (np. usługodawca IT, konsultanci zewnętrzni).
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.
RCPD lub Rejestr oznacza Rejestr Czynności Przetwarzania Danych Osobowych.

5. Ochrona danych osobowych w Kancelarii – zasady ogólne

5.1. Filary ochrony danych osobowych w Kancelarii:

(1) **Legalność** − Kancelaria dba o ochronę prywatności i przetwarza dane zgodnie z prawem.

(2) **Bezpieczeństwo** − Kancelaria zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.

(3) **Prawa Jednostki** − Kancelaria umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.

(4) **Rozliczalność** − Kancelaria dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

5.2. Zasady ochrony danych

Kancelaria 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).

5.3. System ochrony danych

System ochrony danych osobowych w Kancelarii składa się z następujących elementów:

1) **Inwentaryzacja danych.** Kancelaria dokonuje identyfikacji zasobów danych osobowych w Kancelarii, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych, w tym:

   a) przypadków przetwarzania danych specjalnych i danych „kryminalnych" (**dane wrażliwe**);

   b) przypadków przetwarzania danych osób, których Kancelaria nie identyfikuje (**dane niezidentyfikowane**/UFO);

   c) przypadków przetwarzania danych dzieci;

   d) profilowania;

   e) współadministrowania danymi.

   Na dzień 25 maja 2018r. nie stwierdza się przypadków, o których mowa w pkt.a-e.

2) **Rejestr.** Kancelaria opracowuje, prowadzi i utrzymuje Rejestr Czynności Danych Osobowych w Kancelarii (Rejestr). Rejestr jest narzędziem rozliczania zgodności z ochroną danych w Kancelarii.

3) **Podstawy prawne.** Kancelaria zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:

   a) utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikację na odległość,

   b) inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy Kancelaria przetwarza dane na podstawie prawnie uzasadnionego interesu Kancelarii.

4) **Obsługa praw jednostki.** Kancelaria spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:

   a) **Obowiązki informacyjne.** Kancelaria przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków.

   b) **Możliwość wykonania żądań.** Kancelaria weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających.

   c) **Obsługa żądań.** Kancelaria zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO i dokumentowane.

   d) **Zawiadamianie o naruszeniach.** Kancelaria stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

5) **Minimalizacja.** Kancelaria posiada zasady i metody zarządzania minimalizacją (*privacy by default*), a w tym:

a) zasady zarządzania **adekwatnością** danych;

b) zasady reglamentacji i zarządzania **dostępem** do danych;

c) zasady zarządzania okresem **przechowywania** danych i weryfikacji dalszej przydatności;

6) **Bezpieczeństwo.** Kancelaria 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 osób jest wysokie;

c) dostosowuje środki ochrony danych do ustalonego ryzyka;

d) posiada system zarządzania bezpieczeństwem informacji;

e) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych − zarządza incydentami.

7) **Przetwarzający.** Kancelaria posiada zasady doboru przetwarzających dane na rzecz Kancelarii, wymogów co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia.

8) **Eksport danych.** Kancelaria posiada zasady weryfikacji, czy Kancelaria nie przekazuje danych do państw trzecich (czyli poza UE, Norwegię, Lichtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków takiego przekazywania, jeśli ma ono miejsce.

9) ***Privacy by design*.** Kancelaria zarządza zmianami mającymi wpływ na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji w Kancelarii uwzględniają konieczność oceny wpływu zmiany na ochronę danych, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.

10) Przetwarzanie transgraniczne. Kancelaria posiada zasady weryfikacji, kiedy zachodzą przypadki przetwarzania transgranicznego.

6. Inwentaryzacja

6.1. Dane wrażliwe

Kancelaria identyfikuje przypadki, w których przetwarza lub może przetwarzać dane wrażliwe (dane specjalne i dane karne) oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania danych wrażliwych. W przypadku zidentyfikowania przypadków przetwarzania danych wrażliwych, Kancelaria postępuje zgodnie z przyjętymi zasadami w tym zakresie.

6.2. Dane niezidentyfikowane

Kancelaria identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane.

6.3. Profilowanie

Kancelaria identyfikuje przypadki, w których dokonuje profilowania przetwarzanych danych i utrzymuje mechanizmy zapewniające zgodność tego procesu z prawem. W przypadku zidentyfikowania przypadków profilowania i zautomatyzowanego podejmowania decyzji, Kancelaria postępuje zgodnie z przyjętymi zasadami w tym zakresie.

6.4. Współadministrowanie

Kancelaria identyfikuje przypadki współadministrowania danymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami.

7. Rejestr Czynności Przetwarzania Danych

7.1. 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 osobowych, czyli zasady rozliczalności.

7.2. Kancelaria prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.

7.3. Rejestr jest jednym z podstawowych narzędzi umożliwiających Kancelarii rozliczanie większości obowiązków ochrony danych.

8. Podstawy przetwarzania

8.1. Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel Kancelarii) Kancelaria dookreśla podstawę w czytelny sposób, gdy jest to potrzebne. Np. dla zgody wskazując na jej zakres, gdy podstawą jest prawo – wskazując na konkretny przepis i inne dokumenty, np. umowę, porozumienie administracyjne, żywotne interesy – wskazując na kategorie zdarzeń, w których się zmaterializują, uzasadniony cel – wskazując na konkretny cel, np. prowadzenie obsługi księgowej i kadrowo-płacowej, marketing własny, dochodzenie roszczeń.

8.2. Kancelaria wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (email, telefon, sms, in.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).

8.3. Każdy pracownik Kancelarii ma obowiązek znać podstawy prawne, na jakich Kancelaria dokonuje konkretnych czynności przetwarzania danych osobowych. Jeżeli podstawą jest uzasadniony interes Kancelarii, pracownik ma obowiązek znać konkretny realizowany przetwarzaniem interes Kancelarii (obowiązek dotyczy również zleceniobiorców/stażystów/aplikantów/osoby współpracujące).

9. Sposób obsługi praw jednostki i obowiązków informacyjnych

9.1. Kancelaria dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.

9.2. Kancelaria ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: poprzez zamieszczenie na stronie internetowej Kancelarii informacji o przyjętej Polityce ochrony danych.

9.3. Kancelaria dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.

9.4. Kancelaria wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.

9.5. W celu realizacji praw jednostki Kancelaria zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Kancelarię, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany,

10. Obowiązki informacyjne

10.1. Kancelaria określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.

10.2. Kancelaria informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.

10.3. Kancelaria informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.

10.4. Kancelaria informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej.

10.5. Kancelaria określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym).

10.6. Kancelaria informuje osobę o planowanej zmianie celu przetwarzania danych.

10.7. Kancelaria informuje osobę przed uchyleniem ograniczenia przetwarzania.

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

10.9. Kancelaria informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.

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

11. Żądania osób

11.1. **Prawa osób trzecich**. Realizując prawa osób, których dane dotyczą, Kancelaria 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 (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnicę handlową, dobra osobiste itp.), Kancelaria może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

11.2. **Nieprzetwarzanie**. Kancelaria informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.

11.3. **Odmowa**. Kancelaria informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.

11.4. **Dostęp do danych**. Na żądanie osoby dotyczące dostępu do jej danych, Kancelaria informuje osobę, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), 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 Kancelaria nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.

11.5. **Kopie danych**. Na żądanie Kancelaria wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Kancelaria wprowadza i utrzymuje cennik kopii danych, zgodnie z którym pobiera opłaty za kolejne kopie danych. Cena kopii danych skalkulowana jest w oparciu o oszacowany jednostkowy koszt obsługi żądania wydania kopii danych.

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

11.7. **Uzupełnienie danych**. Kancelaria a uzupełnia i aktualizuje dane na żądanie osoby. Kancelaria ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. Kancelaria nie musi przetwarzać danych, które są Kancelarii zbędne). Kancelaria może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Kancelarię procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

11.8. Usunięcie danych. Na żądanie osoby, Kancelaria usuwa dane, gdy:

(1) dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych 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 (np. profil dziecka na portalu społecznościowym, udział w konkursie na stronie internetowej).

Kancelaria 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.

Jeżeli dane podlegające usunięciu zostały upublicznione przez Kancelarię, Kancelaria podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, o potrzebie usunięcia danych i dostępu do nich.
W przypadku usunięcia danych Kancelaria informuje osobę o odbiorcach danych, na żądanie tej osoby.

11.9. Ograniczenie przetwarzania. Kancelaria dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:

a) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,

b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,

c) Kancelaria 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 Kancelarii zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

W trakcie ograniczenia przetwarzania Kancelaria 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.

Kancelaria informuje osobę przed uchyleniem ograniczenia przetwarzania.
W przypadku ograniczenia przetwarzania danych Kancelaria informuje osobę o odbiorcach danych, na żądanie tej osoby.

11.10. Przenoszenie danych. Na żądanie osoby Kancelaria 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 Kancelarii, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Kancelarii.

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

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

11.13. Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu. Jeżeli Kancelaria przetwarza dane w sposób automatyczny, w tym w szczególności profiluje osoby, i w konsekwencji podejmuje względem osoby decyzje wywołujące skutki prawne lub inaczej istotnie wpływające na **osobę**, Kancelaria zapewnia możliwość odwołania się do interwencji i decyzji człowieka po stronie Kancelarii, chyba że taka automatyczna decyzja (i) jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a Kancelarią; lub (ii) jest wprost dozwolona przepisami prawa; lub (iii) opiera się o wyraźną zgodę odwołującej osoby.

12. MINIMALIZACJA

Kancelaria dba o minimalizację przetwarzania danych pod kątem: (i) adekwatności danych do celów (ilości danych i zakresu **przetwarzania**), (ii) dostępu do danych, (iii) czasu przechowywania danych.

12.1. Minimalizacja zakresu

Kancelaria zweryfikowała zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO.
Kancelaria dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.
Kancelaria przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (*privacy by design*).

12.2. Minimalizacja dostępu

Kancelaria stosuje 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).
Kancelaria stosuje kontrolę dostępu fizycznego.
Kancelaria dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających.
Kancelaria dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.
Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w procedurach bezpieczeństwa fizycznego i bezpieczeństwa informacji Kancelaria.

12.3. Minimalizacja czasu

Kancelaria wdraża mechanizmy kontroli cyklu życia danych osobowych w Kancelarii, 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 produkcyjnych Kancelarii, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Kancelarię. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

13. BEZPIECZEŃSTWO

Kancelaria zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Kancelarię.

13.1. Analizy ryzyka i adekwatności środków bezpieczeństwa

Kancelaria przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:

(1) Kancelaria zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania − wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.

(2) Kancelaria kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.

(3) Kancelaria przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Kancelaria 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.

(4) Kancelaria ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym Kancelaria ustala przydatność i stosuje takie środki i podejście jak:

(i) pseudonimizacja,

(ii) szyfrowanie danych osobowych,

(iii) stosowanie antywirusowego oprogramowania Eset klasy Endpoint Security

(iv) inteligentny System firewall z mechanizmem wykrywania incydentów

(v) zarządzanie użytkownikami programów komputerowych oraz dostępami do tych programów i udziałów sieciowych przez wykwalifikowany zespół wsparcia IT, z którym Kancelaria ma zawartą umowę o powierzenie przetwarzania danych

(vi) inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,

(vii) monitoring wizyjny wokół obiektu (lokalu) Kancelarii,

(viii) System wczesnego wykrywania pożaru w lokalu Kancelarii (w tym w archiwum)

(ix) System alarmowy podłączony do systemu monitoringu w agencji ochrony, zabezpieczający lokal Kancelarii przed dostępem osób nieupoważnionych, przed kradzieżą itp.

(x) 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.

13.2. Oceny skutków dla ochrony danych

Kancelaria dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.
Kancelaria stosuje metodykę oceny skutków przyjętą w Kancelarii.

13.3. Środki bezpieczeństwa

Kancelaria 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 Kancelarii i są bliżej opisane w procedurach przyjętych przez Kancelarię dla tych obszarów.

13.4. Zgłaszanie naruszeń

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

14. PRZETWARZAJĄCY

Kancelaria posiada zasady doboru i weryfikacji przetwarzających dane na rzecz Kancelarii 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 Spółce.

Kancelaria przyjęła minimalne wymagania co do umowy powierzenia przetwarzania danych stanowiące Kancelaria rozlicza przetwarzających z wykorzystania podprzetwarzających, jak też z innych wymagań wynikających z Zasad powierzenia danych osobowych.

15. EKSPORT DANYCH

Kancelaria rejestruje w Rejestrze przypadki eksportu danych, czyli przekazywania danych poza Europejski Obszar Gospodarczy (EOG w 2017 r. = Unia Europejska, Islandia, Lichtenstein i Norwegia).
Aby uniknąć sytuacji nieautoryzowanego eksportu danych w szczególności w związku z wykorzystaniem publicznie dostępnych usług chmurowych (shadow IT), Kancelaria okresowo weryfikuje zachowania użytkowników oraz w miarę możliwości udostępnia zgodne z prawem ochrony danych rozwiązania równoważne.

16. PROJEKTOWANIE PRYWATNOŚCI

Kancelaria 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 Kancelarię odwołują się do zasad bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę danych, uwzględnienia i zaprojektowana bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub inwestycji.

Przyjęto do stosowania od dnia 25 maja 2018r.

Ustroń, podpis Joanny Kotarskiej