POLITYKA OCHRONY DANYCH OSOBOWYCH

TAXBOX BIURO RACHUNKOWE

SPIS TREŚCI

- **Administratorem danych osobowych jest TAXBOX BIURO RACHUNKOWE,** zwany dalej „firmą”, „Administratorem”.

KIEDY BIURO RACHUNKOWE JEST ADMINISTRATOREM DANYCH OSOBOWYCH?

W sytuacji, gdy Biuro rachunkowe decyduje o celach i sposobach przetwarzania danych osobowych, czyli **decyduje o tym: jakie dane zbiera** (np. imię, nazwisko, adres zamieszkania), **w jakim celu** (np. cel – realizacja umowy), **jak je będzie przetwarzać i jak zabezpieczać.**

- **Celem Polityki jest zapewnienie właściwej ochrony przetwarzanych danych osobowych.**

CZYM SĄ DANE OSOBOWE?

Są to wszelkie informacje o osobie, które ją identyfikują wprost lub umożliwią jej zidentyfikowanie, np. imię i nazwisko, PESEL, NIP, numer telefonu, adres e-mail, adres zamieszkania / zameldowania / siedziby, numer Klienta, dane o lokalizacji, inne dane określające fizyczną, ekonomiczną, kulturową lub społeczną tożsamość danej osoby.

RODO wyróżnia dane zwykłe i dane szczególnej kategorii (tzw. dane wrażliwe).

CZYM SĄ DANE WRAŻLIWE?

Dane ujawniające pochodzenie rasowe, etniczne, poglądy polityczne, przekonania religijne / światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby oraz dane dot. zdrowia, seksualności, orientacji seksualnej.

- Wprowadzenie Polityki zostało poprzedzone dokonaniem ogólnej oceny ryzyka w zakresie przetwarzania danych osobowych oraz przeprowadzeniem wewnętrznego audytu oraz weryfikacją tego czy potrzebny jest Inspektor Ochrony Danych Osobowych.

I. NAJWAŻNIENIE ZASADY DOT. OCHRONY DANYCH OSOBOWYCH

PODSUMOWANIE:

- **Biuro nie zbiera danych „na wszelkich wypadek" lub „bo może kiedyś się przydadzą do innego celu".** Należy dbać o to, żeby dane były zbierane **w niezbędnej ilości** i **w zakresie,** a także przechowywane **przez czas niezbędny do realizacji celu i gdy mamy do tego podstawę prawną.**

  Przykład: jeśli do wykonywania danej pracy, wizerunek nie jest istotną cechą, nie można w ogłoszeniu rekrutacyjnym wymagać od kandydatów „wysyłania CV ze zdjęciem". Ponadto, po przeprowadzeniu rekrutacji, przesłane CV powinny być co do zasady niezwłocznie usunięte, chyba że planowana jest kolejna rekrutacja, a kandydaci wyrazili zgodę na udział w kolejnych rekrutacjach.

- **Biuro rachunkowe chroni dane przy użyciu odpowiednich środków bezpieczeństwa**.
  Przykład:
  1) odpowiednie oprogramowanie antywirusowe / firewall, itp.
  2) niepozostawianie danych w miejscu, do którego inni mają swobodny dostęp
  3) stosowanie silnych haseł lub innych zabezpieczeń do komputera / laptopa / dysku lub korzystanie z managera haseł, itp.

- **Biuro rachunkowe stosuje się do zaleceń wskazanych w dokumencie**: „**Zasady pracy zgodnie z RODO"** (załącznik nr 1).

- **Biuro rachunkowe informuje osoby o zasadach przetwarzania ich danych osobowych** *(np. poprzez umieszczenie odpowiednich informacji w Polityce prywatności, stopce e-maila, poprzez przekazywanie ww. informacji przy okazji zawierania umów).*

- **Biuro rachunkowe odpowiada na prośby / pytania / wnioski osób, których dane posiada / zbiera. Wdrożono w tym zakresie „Procedurę dot. obsługi żądań ww. osób"** (załącznik nr 2).

- **W przypadku, gdy podmiot trzeci (poza Administratorem) ma mieć dostęp do danych osobowych należy wydać mu upoważnienie lub zawrzeć z nim umowę powierzenia,** chyba że zachodzi inna sytuacja wynikająca m.in. z przepisów prawa.

ZASADY DOT. PRZETWARZANIA DANYCH

1. **Biuro rachunkowe zapewnia przetwarzanie danych osobowych zgodnie z RODO**, tj.
   1) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
   2) rzetelnie i uczciwie (rzetelność);
   3) w konkretnych celach, nie „na zapas” (minimalizacja);
   4) nie więcej niż potrzeba (adekwatność);
   5) z dbałością o prawidłowość danych (prawidłowość);
   6) nie dłużej niż potrzeba (czasowość);
   7) zapewniając odpowiednie bezpieczeństwo danych i wprowadzając odpowiednie środki techniczne i organizacyjne (bezpieczeństwo), m.in. poprzez wprowadzenie *Zasad pracy zgodnych z RODO – załącznik do Polityki* (w tym w zakresie systemów informatycznych i Polityki czystego biurka);
   8) spełniając obowiązki informacyjne względem osób, których dane przetwarza;
   9) umożliwiając osobom, których dane dotyczą wykonywania swoich praw; wprowadzono *Procedurę obsługi żądań ww. osób - załącznik do Polityki;*
   10) zapewniając rozliczalność, w celu wykazania zgodności wypełniania obowiązków RODO.

PODSTAWA PRZETWARZANIA DANYCH

2. **Przetwarzanie przez Biuro rachunkowe jest zgodne z prawem** m.in. gdy:
   1) osoba, której dane dotyczą **wyraziła zgodę** na przetwarzanie danych (np. do celów przyszłych rekrutacji lub zgodę na przetwarzanie danych wrażliwych, np. dot. zdrowia);
   2) przetwarzanie jest **niezbędne do wykonania umowy** (np. realizacji zamówienia, realizacji umowy zlecenia, umowy o pracę) lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy (np. do przygotowania oferty, do przeprowadzenia prezentacji produktu);
   3) przetwarzanie jest niezbędne do **wypełnienia obowiązków prawnych** nałożonych na Administratora (m.in. do celów archiwizacyjnych, podatkowych np. przechowywanie faktury czy dokumentacji pracowniczej, ale także w celu przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu);
   4) wynika to z **prawnie uzasadnionych interesów** realizowanych przez Administratora (np. dochodzenie i obrona przed roszczeniami, marketing bezpośredni);
   5) wynika to z innej podstawy prawnej przewidzianej przepisami RODO.

PRZETWARZANIE DANYCH W ZWIĄZKU Z USTAWĄ O PRZECIWDZIAŁANIU PRANIU PIENIĘDZY I FINANSOWANIU TERRORYZMU

3. Biuro rachunkowe przekazuje Klientom klauzulę informacyjną uwzględniającą to, że dane zbierane są także w celu realizacji obowiązków prawnych związanych z ustawą o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu.
4. Biuro rachunkowe uwzględnia przetwarzanie danych do celów wskazanych powyżej w rejestrze czynności przetwarzania.
5. Zakres gromadzonych i przetwarzanych danych, a także sposób ich wykorzystywania i długość okresu muszą być adekwatne do celu.
6. Biuro rachunkowe jest uprawnione, aby w ramach stosowanych środków bezpieczeństwa finansowego przetwarzać informacje zawarte w dokumentach tożsamości klienta i osoby upoważnionej do działania w jego imieniu oraz sporządzać ich kopie.
7. Biuro rachunkowe zapewnia szkolenie uwzględniające przetwarzanie danych w oparciu o ustawę o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu.
8. Termin przechowywania danych zostanie określony w Procedurze z zakresu przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu.

ŚRODKI TECHNICZNE I ORGANIZACYJNE

9. Dane osobowe są chronione przy zastosowaniu zabezpieczeń niezbędnych dla zapewnienia poufności, integralności, dostępności i rozliczalności danych osobowych. **Biuro rachunkowe przeprowadza m.in.:**
   1) audyt oraz **analizę ryzyka** dla czynności przetwarzania danych / kategorii;
   2) wprowadza **niezbędne procedury i regulacje** (m.in. wprowadza niniejszą Politykę, procedurę zgłaszania naruszeń, upoważnienia);
   3) zarządza zmianami mającymi wpływ na prywatność. Administrator stosuje politykę *privacy by design i privacy by default - załącznik do Polityki (Procedura dot. ochrony danych w wersji BETA (Polityka privacy by design i privacy by default);*
   4) wykonuje inne obowiązki wynikające z przepisów obowiązującego prawa.
10. W przypadku, gdy podmiot trzeci ma dostęp do danych powinno zostać wydane *upoważnienie do przetwarzania danych* (załącznik do Polityki) lub powinna zostać zawarta *umowa powierzenia* (więcej w pkt III Polityki ochrony danych).
11. Biuro rachunkowe umożliwia osobom, których dane dotyczą, zapoznanie się z informacjami dot. przetwarzania ich danych osobowych.

Załączniki do Polityki ochrony danych, o których mowa w rozdziale:

- Zasady pracy zgodnie z RODO
- Procedura obsługi żądań ww. osób
- Polityka privacy by design i privacy by default

- Upoważnienie do przetwarzania danych
- Umowa powierzenia

II. REJESTR CZYNNOŚCI PRZETWARZANIA – PODSTAWOWY DOKUMENT OPISUJĄCY JAKIE DANE BIURO RACHUNKOWE PRZETWARZA

PODSUMOWANIE:

- **W Rejestrze czynności przetwarzania wskazuje się procesy w Biurze rachunkowym, w których dochodzi m.in. do zbierania (przetwarzania) danych osobowych** (np. proces związany z obsługą potencjalnych Klientów, proces związany z obsługą Klientów (tj. umów / zamówień).
- **W przypadku, gdy po dniu stworzenia rejestru czynności pojawi się nowy proces**, **należy ten Rejestr uzupełnić o nowy proces.**

1. Biuro rachunkowe prowadzi Rejestr czynności przetwarzania, w którym opisuje procesy, jakie zachodzą w Biurze rachunkowym, w ramach których dochodzi do zbierania i innego przetwarzania danych.
2. Rejestr stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację zasady rozliczalności.
3. Rejestr należy systematycznie weryfikować i ewentualnie aktualizować.

Załączniki do Polityki ochrony danych, o których mowa w rozdziale:

- Rejestr czynności przetwarzania

III. UMOWA POWIERZENIA – JAKO DOKUMENT PRZEKAZANIE DANYCH

PODSUMOWANIE:

- Z uwagi na specyfikę prowadzonej działalności, Biuro otrzymuje do przetwarzania dane osobowe od swoich Klienta (m.in. dane jego kontrahentów, dane pracowników).
- W związku z tym, przy zawieraniu umów o współpracę z Klientem, należy zawierać również umowę powierzenia przetwarzania danych osobowych.
- Umowę można sporządzić w oparciu o wzór umowy powierzenia oraz zgodnie z instrukcją stanowiącą załącznik do Polityki ochrony danych;
- Każda umowa powinna zostać wskazana w Rejestrze kategorii przetwarzań.
- W przypadku, gdy Biuro rachunkowe przekazuje innej firmie dane, które co do zasady „zbiera samodzielnie" (np. dane Klientów, dane subskrybentów newslettera, potencjalnych Klientów) należy zawrzeć umowę powierzenia.
- Przykłady podmiotów, z którymi należy zawrzeć umowę powierzenia, jeśli taka współpraca zostanie nawiązana: firma hostingowa, wirtualna asystentka, podmiot obsługujący newsletter, firma prowadząca monitoring, podmioty, które współpracującą przy realizacji zleceń i otrzymują dane osobowe.

- **Ważne**! Przekazanie danych firmie specjalistycznej nie zwalnia Administratora, tj. Biuro rachunkowe z odpowiedzialności w przypadku, gdy dojdzie do naruszenia ochrony przekazanych danych. Warto więc wybierać firmy do współpracy, które dbają o ochronę danych.

UMOWA POWIERZENIA

1. Umowa powierzenia reguluje współpracę między Biurem Rachunkowym, a firmą zewnętrzną / Klientem. Wzór umowy – załącznik do Polityki.
2. W umowie opisano zasady, w oparciu o które podmiot otrzymujący dane może działać, tj. m.in. zasady korzystania z danych, zabezpieczania danych, dalszego przekazywania itp.
3. W przypadku gdy Biuro rachunkowe przekazuje innym podmiotom dane do przetwarzania, przed zawarciem umowy powierzenia, Biuro rachunkowe m.in. weryfikuje czy:
   1) podmiot przetwarzający zapewnia gwarancję należytego przetwarzania powierzonych danych, tj. czy dba o dane osobowe zgodnie z RODO,
   2) umowa powierzenia zawiera wszystkie elementy przewidziane art. 28 RODO (jeżeli nie została stworzona w oparciu o wzór stanowiący załącznik do Polityki),
   3) nie zachodzi konieczność dodatkowych zabezpieczeń umowy.

REJESTR KATEGORII PRZETWARZANIA (dot. sytuacji, gdy Biuro rachunkowe otrzymuje dane od innego podmiotu trzeciego)

1. W przypadku, gdy to Biuro rachunkowe otrzymuje dane osobowe do przetwarzania od podmiotu trzeciego – zawiera z nim umowę powierzenia.
2. Przekazanie danych od innych podmiotów należy wskazać w Rejestrze Kategorii przetwarzań.

Załączniki do Polityki ochrony danych, o których mowa w rozdziale:

- Umowa powierzenia wraz z instrukcją
- Rejestr kategorii przetwarzań

IV. UDOSTĘPNIANIE DANYCH BEZ KONIECZNOŚCI ZAWIERANIA UMOWY POWIERZENIA

1. Otrzymując od organu państwowego (np. ZUS, US, sądy) lub innego podmiotu wniosek o udostępnienie danych, należy sprawdzić czy istnieje podstawa prawna takiego wniosku i czy została w takim wniosku wskazana.
2. Dane bez umowy powierzenia udostępniane są także innym podmiotom, które są do tego uprawnione, jak np. Poczta Polska, banki.
3. W przypadku, gdy brak jest takiej podstawy, należy wezwać do wskazania takiej podstawy prawnej, a jeśli nie zostanie wskazana - odmówić udostępnienia danych.
4. Inne przypadki udostępnienia danych muszą być każdorazowo weryfikowane co do podstaw prawnych takiego udostępnienia.
5. Należy odnotowywać takie udostępnienie danych.

V. ZGŁASZANIE NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

PODSUMOWANIE:

W przypadku wystąpienia incydentu / naruszenia ochrony danych należy zastosować Procedurę zgłoszenia naruszeń opisaną w załączniku do Polityki.

1. Biuro rachunkowe stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od stwierdzenia naruszenia zgodnie z załącznikiem do niniejszej Polityki.
2. Biuro rachunkowe prowadzi Rejestr naruszeń, w którym opisuje wszystkie naruszenia ochrony danych, jakie wystąpiły.

Załączniki do Polityki ochrony danych, o których mowa w rozdziale:

- Procedura zgłaszania naruszeń wraz z Rejestrem naruszeń

VI. MONITOROWANIE

Biuro rachunkowe dba o to, żeby zasady ochrony danych były przestrzegane w toku jej działalności. Zaleca się, aby audyt i analiza ryzyka dotycząca właściwej ochrony danych były przeprowadzane nie rzadziej niż raz na 2 lata lub w razie potrzeby – częściej.

VII. PRZEKAZYWANIE DANYCH DO PAŃSTW TRZECICH

W przypadku, gdy zachodzi przekazanie danych do państw trzecich poza EOG, Biuro rachunkowe dokonuje przekazania w oparciu o gwarancje wynikające z RODO, tj. m.in. w oparciu o standardowe klauzule umowne lub bez ww. zabezpieczeń w oparciu o zgodę osoby, której dane dotyczącą lub też w oparciu o inne przesłanki przewidziane w RODO (m.in. niezbędność do zawarcia / realizacji umowy).

VIII. WSPÓŁADMINISTROWANIE o ile dotyczy

1. W przypadku, gdy zachodzi współadministrowanie, tzn. poza Biurem rachunkowym również inny podmiot decyduje o celach przetwarzania danych i środkach ich zabezpieczania (np. dwie firmy razem są współorganizatorami jakiegoś przedsięwzięcia), informacja o współadministrowaniu wskazywana jest w:
   1) klauzulach informacyjnych,

2) rejestrze czynności przetwarzania.

2. W związku ze współadministrowaniem zawierana jest także umowa o współadministrowanie.

IX. OBOWIĄZKI OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH (NP. PRACOWNIKÓW)

1. Dane osobowe mogą być przetwarzane wyłącznie w oparciu o upoważnienie do przetwarzania wydane przez Biuro rachunkowe. Wzór upoważnienia i oświadczenia stanowi załącznik do Polityki.

2. Każda osoba, która uzyskała upoważnienie do przetwarzania danych osobowych zobowiązana jest do:

   1) przetwarzania ich co do zasady wyłącznie na polecenie Biura rachunkowego;

   2) ochrony danych w sposób zgodny z przepisami prawa i wewnętrznymi zaleceniami;

   3) zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczania.

3. Podczas przetwarzania danych trzeba zachować szczególną ostrożność i podjąć wszelkie możliwe środki umożliwiające zabezpieczenie oraz ochronę danych przed nieuprawnionym dostępem, modyfikacją, utratą, zniszczeniem lub ujawnieniem.
4. Biuro rachunkowe prowadzi ewidencję upoważnień. Wzór – załącznik do Polityki

---

Załączniki do Polityki ochrony danych osobowych, o których mowa w rozdziale:

- Upoważnienie wraz z oświadczeniem
- Ewidencja upoważnień

X. POSTANOWIENIA KOŃCOWE

1. Dokumentacja przetwarzania danych osobowych stanowi wewnętrzną regulację Biura rachunkowego i obowiązuje wszystkich pracowników i współpracowników Biura oraz inne osoby przetwarzające dane osobowe przetwarzane przez Biuro.

2. Dokumentacja przetwarzania danych osobowych obowiązuje od dnia jej wprowadzenia w życie w sposób przyjęty przez Biuro rachunkowe.
3. W sprawach nieuregulowanych mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym w szczególności przepisy ustawy i Rozporządzenia Ogólnego.

XI. NAJWAŻNIEJSZE POJĘCIA

1. **Dane osobowe** oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą");
2. **Integralność i poufność** oznacza przetwarzanie w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową ich utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych;
3. **Naruszenie ochrony danych osobowych** oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
4. **Podmiot przetwarzający** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;
5. **Przetwarzanie** oznacza operację lub zestaw operacji wykonywanych na danych osobowych takich jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
6. **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);
7. **Ustawa** oznacza ustawę o ochronie danych osobowych z dnia 10 maja 2018r.;
8. **Zbiór danych** oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
9. **Zgoda osoby, której dane dotyczą** oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

XII. ZAŁĄCZNIKI

- Zasady pracy zgodnie z RODO
- Procedura zgłaszania naruszeń wraz z Rejestrem
- Procedura obsługi wniosków i żądań osób, których dane dotyczą
- Procedura dot. ochrony danych w wersji BETA (Polityka privacy by design i privacy by default)
- Rejestr czynności przetwarzania
- Umowa powierzenia wraz z instrukcją
- Rejestr kategorii przetwarzań
- Upoważnienie wraz z oświadczeniem
- Ewidencja upoważnień