KLAUZULA INFORMACYJNA - POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Kancelaria Adwokacka Adwokat Michał Orlikowski

Informacja o administratorze danych osobowych

Administratorem Państwa danych osobowych jest Kancelaria Adwokacka Adwokat Michał Orlikowski z siedzibą w Warszawie przy pl. Mirowskim 12/19, (00-138 Warszawa) NIP: 9591870305, zwany dalej „Administratorem". Dane osobowe są przetwarzane w biurze w siedzibie firmy.

Zasady ogólne dotyczące bezpieczeństwa przetwarzanych danych osobowych

Cel Polityki

Celem opracowania i wprowadzenia niniejszej Polityki jest opisanie zastosowanych wewnątrz Kancelaria Adwokacka Adwokat Michał Orlikowski z siedzibą w Warszawie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, odpowiednich do ryzyka naruszenia praw i wolności w związku z przetwarzaniem danych osobowych. Polityka została opracowana stosownie do przepisów 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. Niniejszy dokument będzie wdrożony poprzez jego publiczny dostęp oraz zapoznawania z nim osób upoważnionych do przetwarzania danych osobowych, a także innych osób mających dostęp do danych osobowych przetwarzanych przez Administratora.

Poniżej znajdziesz wszelkie niezbędne informacje dotyczące przetwarzania danych osobowych w związku z realizacją zatrudnienia lub współpracy.

Definicje

Określenia użyte w Polityce oznaczają:

1. Administrator	przedsiębiorstwo Kancelaria Adwokacka Adwokat Michał Orlikowski z siedzibą w Warszawie przy pl. Mirowskim 12/19, (00-138 Warszawa) NIP: 9591870305- w odniesieniu do danych osobowych, co do których decyduje o celach przetwarzania;
2. Dane osobowe	wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden

	bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
3. Dane osobowe zwykłe	wszystkie dane osobowe niewchodzące w zakres danych osobowych wrażliwych;
4. Dane osobowe wrażliwe (znajdujące się w katalogu danych w art. 9 ust. 1 RODO)	dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby oraz dane wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa;
5. Prezes urzędu	Prezes Urzędu Ochrony Danych Osobowych;
6. Hasło	ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
7. Identyfikator użytkownika	ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
8. Integralność danych	właściwość wskazująca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
9. Incydent bezpieczeństwa	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;
10. Odbiorca	oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania
11. Osoba upoważniona	oznacza osobę posiadającą upoważnienie do przetwarzania danych osobowych;
12. Właściciel danych	każda osoba fizyczna, której dane osobowe są przetwarzane przez „Administratora” lub na zlecenie „Administratora” w związku z prowadzoną przez nią działalnością;
13. Poufność danych	właściwość wskazująca, że dane nie są udostępniane nieupoważnionym podmiotom,

14. Pracownik	osoba, posiadająca dostęp do danych osobowych, świadcząca pracę na rzecz „Administratora” na podstawie stosunku pracy;
15. Strona trzecia	oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, innego administratora, podmiot przetwarzający czy osoby, które – z upoważnienia „Administratora” lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;
16. Procesor	osoba prawna, osoba fizyczna, jednostka organizacyjna nieposiadająca osobowości prawnej lub inny podmiot, który nie decyduje o celach i środkach przetwarzania danych osobowych, któremu EGC powierzyło do przetwarzania dane osobowe oraz zawarł Umowę powierzenia przetwarzania danych osobowych w rozumieniu art. 28 RODO;
17. Przetwarzanie danych osobowych	oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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;
18. Polityka	niniejszy dokument - Polityka bezpieczeństwa danych osobowych prowadzonej przez „Administratora”
19. Rozliczalność (art. 5 ust. 2 Ustawy RODO)	właściwość umożliwiająca wykazanie zgodności działalności Administratora z przepisami RODO;
20. RODO lub Rozporządzenie	Rozporządzenie 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;
21. Skarga	jakiekolwiek pismo (w postaci papierowej lub elektronicznej) przekazane przez podmiot danych (właściciela danych) lub Prezesa Urzędu, z treści którego wynika niezadowolenie lub żądanie wyjaśnień / informacji dotyczących przetwarzania danych osobowych przez Administratora;
22. System informatyczny (lub system IT)	zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
23. Teletransmisja	przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej zgodnie z definicją zawartą w art. 2 pkt 29 Ustawy z dnia 16 lipca 2004 roku Prawo telekomunikacyjne.
24. Ustawa	Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych
25. Upoważnienie	jedno z poniższych:

	- pisemne upoważnienie wydane na podstawie art. 29 RODO do przetwarzania danych osobowych nadane Pracownikowi, Współpracownikowi lub pracownikowi Procesora przez „Administratora”, - Umowa powierzenia przetwarzania danych osobowych zawarta na piśmie rozumieniu art. 28 RODO;
26. Usuwanie danych	oznacza trwałe i nieodwracalne zniszczenie danych osobowych lub taka ich modyfikacja, w taki sposób, aby nie było możliwe ich dalsze przetwarzanie, odtworzenie ani identyfikacja osoby, której dane dotyczą, przy użyciu dostępnych środków technicznych i organizacyjnych. Usunięcie danych obejmuje zarówno skasowanie danych z systemów informatycznych, baz danych i nośników elektronicznych, jak również zniszczenie dokumentów w formie papierowej, zgodnie z obowiązującymi przepisami prawa oraz przyjętymi procedurami bezpieczeństwa.
27. Uwierzytelnianie	działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
28. Użytkownik systemu IT	użytkownik systemu informatycznego, któremu nadano prawa dostępu do dowolnego systemu informatycznego należącego do „Administratora” lub z którego „Administrator” korzysta z zachowaniem przepisów ROOD;
29. Współpracownik	osoba, posiadająca dostęp do danych osobowych wykonująca osobiście i bezpośrednio zadania / usługi na rzecz Administratora na innej podstawie prawnej niż stosunek pracy, bez względu na nazwę lub rodzaj łączącej strony umowy;
30. Zabezpieczenie danych	wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
31. Zewnętrzne narzędzie informatyczne	oznacza system lub aplikację informatyczną udostępnianą Administratorowi przez podmiot trzeci, niewchodzącą w skład infrastruktury Administratora, wykorzystywaną do gromadzenia, zapisywania i przechowywania danych osobowych w formie elektronicznej w sposób zapewniający integralność i bezpieczeństwo danych osobowych (np. formularze SurveyLab, Google)
32. Zgoda osoby, której dane dotyczą	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;

Obowiązki Administratora

Obowiązek spełnienia podstaw prawnych dla przetwarzania danych osobowych

Każdy Pracownik lub Współpracownik przed podjęciem decyzji o utworzeniu celu przetwarzania lub poszerzenia zakresu zbieranych danych osobowych do aktualnego celu przetwarzania jest zobowiązany do ustalenia i wskazania podstawy prawnej (art. 6 i nast. RODO)

Obowiązek informacyjny w stosunku do podmiotu danych (art. 13 i art. 14):

1) Każdy Pracownik i Współpracownik który zbiera (pozyskuje) dane osobowe, w momencie ich zbierania bezpośrednio od właściciela danych, jest zobowiązany poinformować właściciela danych o tym fakcie;

2) przypadku zbierania danych od osób trzecich, właściciela danych należy poinformować niezwłocznie po utrwaleniu danych o okolicznościach przetwarzania w zgodzie z wymaganiami RODO.

3) W przypadku korzystania z systemów informatycznych, które automatycznie zbierają dane osobowe, należy zapewnić, aby system ten udzielał informacji, o których mowa w punktach powyżej 1) i 2).

4) **W przypadku korzystania z podmiotów trzecich należy zapewnić w umowie z takim podmiotem, aby w trakcie zbierania danych osobowych, podmiot ten wykonywał obowiązek informacyjny w jego imieniu zgodnie z punktem 1) i 2).**

Obowiązek przestrzegania zasad przetwarzania (art. 5 RODO).

W trakcie procesów przetwarzania danych osobowych należy dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, w szczególności przestrzegania zasad określonych w niniejszej Polityce. Obowiązek ten dotyczy zarówno Pracowników i Współpracowników Administratora jak i podmiotów, które w imieniu Administratora przetwarzają dane osobowe.

Obowiązek zawarcia umowy powierzenia przetwarzania danych osobowych (art. 28 RODO)

Jeśli Administrator podejmie decyzję o korzystaniu z usług podmiotu trzeciego, a w ramach świadczenia tych usług podmiot ten będzie przetwarzał dane osobowe na zlecenie lub w imieniu Administratora, należy zapewnić, aby przed przekazaniem danych temu podmiotowi, została zawarta „Umowa powierzenia przetwarzania danych osobowych" zgodnie z zasadami określonymi w punkcie niniejszej Polityce.

Obowiązek realizacji żądań osoby, której dane dotyczą

1) Jeśli właściciel danych zgłosi się z ustnym lub pisemnym wnioskiem / prośbą o dostęp / kopię danych / przeniesienie danych / usunięcie jego danych / sprostowanie / ograniczenie / zaktualizowanie (niezależnie od formy zgłoszenia papierowo lub elektronicznie) należy niezwłocznie, maksymalnie w ciągu 30 dni, zrealizować taki wniosek, jeśli jest zasadny.

2) Pracownik lub Współpracownik wskazany do realizacji takiego wniosku ułatwia osobie, której dane dotyczą, wykonanie praw przysługujących jej na mocy art. 15–22 RODO.

3) Każdy Pracownik i Współpracownik jest zobowiązany stosować zabezpieczenia:

    a) organizacyjne (np. polityki, regulaminu, procedury) obowiązujące u Administratora niezależnie do tego jakim dokumentem wewnętrznym zostały one opisane oraz

    b) techniczne (np. stosowanie haseł dostępowych). Obchodzenie zabezpieczeń określonych w dokumentach wewnętrznych lub wdrożonych przez dostawcę IT może stanowić incydent bezpieczeństwa w zakresie ochrony danych osobowych. Obowiązek zabezpieczenia danych dotyczy również Procesorów. Szczegółowe wymagania odnośnie zabezpieczania danych osobowych przez procesora powinny być określone w „Umowie powierzenia przetwarzania danych osobowych"

Obowiązki i odpowiedzialność

Obowiązki i odpowiedzialność wszystkich Pracowników i Współpracowników

Każdy Pracownik i Współpracownik, niezależnie od stanowiska czy zadań jest zobowiązany do i odpowiada za:

1) zachowanie w poufności danych osobowych oraz sposobu ich zabezpieczeń,
2) zapoznanie i stosowanie się do zapisów niniejszej Polityki oraz dokumentów wewnętrznych wydanych na podstawie niniejszej Polityki i pozostałej dokumentacji z zakresu RODO
3) pisemne potwierdzenie zapoznania się z przepisami o ochronie danych osobowych i niniejszą Polityką
4) przestrzeganie przepisów o ochronie danych osobowych w szczególności Ustawy,
5) trzymanie pełnej poufności swoich haseł do systemów IT,
6) przestrzeganie zakazu dostępu do danych osobowych osobom nieupoważnionym,
7) zgłaszanie każdego podejrzenia incydentu bezpieczeństwa dot. danych osobowych, w tym niniejszej Polityki Administratorowi.

Obowiązki i odpowiedzialność w zakresie systemów IT

Każdy pracownik i współpracownik we współpracy z Administratorem jest zobowiązany do i odpowiada za:

1) wdrożone i utrzymywane zabezpieczeń (fizycznych, logicznych, systemowych) oraz nadzorowanie ich skuteczności,
2) nadzorowanie czy wdrożone ograniczenia dostępów do obszarów przetwarzania danych są skuteczne,
3) uwzględnianie przepisów RODO oraz Polityki w trakcie projektowania i wdrażania nowych rozwiązań dotyczących bezpieczeństwa informatycznego lub fizycznego,

4) na wniosek Administratora - współpracownik sporządzania informacje dotyczących stosowanych zabezpieczeń.

Zasady postępowania w przypadku skarg na przetwarzanie danych osobowych

Skargi / wnioski wnoszone przez właściciela danych

1) W przypadku pisemnej skargi / wniosku (niezależnie od formy doręczenia czy zatytułowania) przesłanej przez właściciela danych do Administratora należy taką skargę / wniosek rozpatrzyć niezwłocznie, nie dłużej niż w terminie nie przekraczającym 30 dni od daty wpłynięcia.
2) Odpowiedź na skargę / wniosek należy udzielić na piśmie (z pocztowym potwierdzeniem odbioru) jeśli wnoszący podał adres do doręczeń, natomiast w przypadku braku takiego adresu tą samą drogą, którą skarga / wniosek został złożona, chyba, że wnioskujący poprosił o inną formę.
3) Jeśli właściciel danych zgłosi się z wnioskiem, prośbą o zmianę lub aktualizację danych osobowych, należy uczynić to niezwłocznie po uzyskaniu takiego wniosku.
4) Jeśli właściciel danych zgłosi się z wnioskiem, prośbą o usunięcie lub zaprzestania przetwarzania jego danych, a dane te były zbierane tylko na podstawie zgody tej osoby, należy usunąć niezwłocznie jego dane osobowe lub zaprzestać przetwarzania do celów na jakie wyraził wcześniej zgodę.
5) Dane osobowe przetwarzane na podstawie zawartej umowy, po odwołaniu wszystkich zgód właściciela danych, mogą być nadal wykorzystywane w innych celach (np. wykonanie umowy, podatkowe), jeśli takowe wynikają z potrzeby zakończenia lub rozliczenia wykonania umowy.
6) Jeśli właściciel danych zgłosi się z wnioskiem o dostęp do jego danych osobowych lub uzyskanie kopii danych to na taki wniosek należy odpowiedzieć niezwłocznie, nie przekraczając 30 dni.

Skargi przekazywane przez Prezesa Urzędu

W przypadku skargi złożonej przez właściciela danych do Prezesa Urzędu, które organ przekazał do Administratora, Administrator niezwłocznie udzieli odpowiedzi na taką skargę doręczoną przez Prezesa w terminie 7 dni (chyba, że Prezes Urzędu wyznaczy inny termin).

Zasady przetwarzania danych osobowych przez Administratora

Zasada legalności, rzetelności i przejrzystości

Dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą. Nie wolno przetwarzać danych osobowych bez podstawy prawnej. Przed przystąpieniem do przetwarzania nowej kategorii danych osobowych lub danych w nowym celu należy wskazać podstawę prawną do ich przetwarzania.

Zasada minimalizacji danych

Dane osobowe muszą być przetwarzane wyłącznie w konkretnym i jasno sprecyzowanym celu, a właściciel danych musi być o tym celu poinformowany. Dane osobowe musza być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami. Można zbierać tylko tyle danych, ile jest adekwatne do realizacji celu. Dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

Zasada prawidłowości

Wszystkie osoby upoważnione do przetwarzania i Procesorzy odpowiadają za poprawność merytoryczną danych. Dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.

Zasada ograniczenia przetwarzania

Można przetwarzać dane osobowe tylko tak długo jak długo istnieje cel przetwarzania lub określają to przepisy prawa. Dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.

Zasada poufności i integralność

Dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

Zasada zaznajamiania osób upoważnionych z przepisami wewnętrznymi i zewnętrznymi w zakresie ochrony danych osobowych

Każda osoba upoważniona do przetwarzania danych osobowych (każdy Pracownik i Współpracownik) jest zobowiązany do zapoznawania się na bieżąco z przepisami wewnętrznymi i zewnętrznymi w zakresie ochrony danych osobowych. Każda osoba upoważniona po zapoznaniu się z przepisami i zasadami w zakresie ochrony danych osobowych, potwierdza ten fakt poprzez pisemne podpisanie stosownego oświadczenia.

Zasada ograniczonego dostępu

Dostęp do danych osobowych zawsze musi być ograniczony tylko dla osób upoważnionych. Ograniczanie dostępu może być organizacyjne (np. osobiste nadzorowanie, wprowadzanie procedur), fizyczne (np. zamykanie na klucz) lub informatyczne (np. stosowanie loginów haseł).

Zasada rozliczalności

1) Działania osoby upoważnionej lub Procesora na danych osobowych w szczególności w systemach informatycznych muszą być zawsze przypisane w sposób jednoznaczny tylko jednemu Pracownikowi. To oznacza, że dany login do systemu IT może być przypisany tylko jednej osobie. Zakazane jest współdzielenie loginów przez dwie i więcej osób. Pod żadnym pozorem pracownik/współpracownik/osoba upoważniona lub Procesor nie może ujawnić

swojego hasła dostępowego dosystemu zawierającego dane osobowe którego administratorem jest Administrator.

2) Wykonując obowiązki i zadania z przepisów RODO oraz niniejszej Polityki, każda osoba upoważniona jest zobowiązana wykazać, że przestrzega przepisów RODO i Polityki.

Zasady powierzania przez Administratora przetwarzania danych osobowych podmiotom trzecim

Stosowanie umów powierzenia

W przypadku zawierania umowy o świadczenie usług, które jest związane z powierzeniem przetwarzania danych osobowych dostawcy usługi, należy zawrzeć pisemną umowę powierzenia przetwarzania zgodną z art. 28 RODO.

Obowiązki i odpowiedzialności Procesorów

W trakcie tworzenia umowy powierzenia przetwarzania danych osobowych należy bezwzględnie ująć w niej elementy wynikające z przepisów RODO w tym zakresie, w szczególności wskazać w umowie przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa Administratora oraz Procesora. Umowa powinna nadto stanowić, że:

a) Procesor przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny,

b) Procesor zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,

c) Procesor podejmuje wszelkie środki wymagane na mocy art. 32 RODO,

d) Procesor nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian,

e) jeżeli do wykonania w imieniu Administratora konkretnych czynności przetwarzania Procesor korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego

   – te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między administratorem a podmiotem przetwarzającym, o których to obowiązkach mowa powyżej,

w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom niniejszego rozporządzenia.

- jeżeli ten inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na pierwotnym podmiocie przetwarzającym,

f) Procesor biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w Rozdziale III RODO,

g) Procesor uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO,

h) Procesor po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych,

i) Procesor udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych art. 28 RODO oraz umożliwia Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

Kontrola Procesorów

W każdej umowie powierzenia przetwarzania danych osobowych, obowiązkowo stosuje się zapis o możliwości przeprowadzenia kontroli (audytu) zgodności przetwarzania powierzonych danych z Umową oraz przepisami.

Wykorzystanie Zewnętrznych Narzędzi Informatycznych

Administrator może wykorzystywać zewnętrzne narzędzie informatyczne służące do gromadzenia danych jako pomocniczą formę przyjmowania zgłoszeń. Korzystanie z tego narzędzia jest dobrowolne, a Administrator zapewnia alternatywną formę przekazania danych. W związku z korzystaniem z zewnętrznego narzędzia informatycznego dane osobowe mogą być przekazywane do państw trzecich poza Europejskim Obszarem Gospodarczym. Przekazywanie danych odbywa się zgodnie z zasadami określonymi w rozdziale V Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO), w szczególności na podstawie standardowych klauzul umownych, o których mowa w art. 46 RODO."

Umowa powierzenia (Art. 28 RODO) – Google oferuje tzw. „Data Processing Terms" dla Google Workspace, które formalnie powierza przetwarzanie danych w imieniu administratora. Należy upewnić się, że zawarcie takiej umowy jest możliwe i aktywne w Twoim przypadku.

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Środki organizacyjne i techniczne zabezpieczenia danych osobowych

W celu wzmocnienia nadzoru nad procesami przetwarzania danych osobowych zostały wprowadzone środki organizacyjne i techniczne zabezpieczenia danych opisane w niniejszym punkcie.

Środki ochrony fizycznej

1) Biuro w którym znajdują się pomieszczenia, w których przetwarzane są zbiory danych osobowych objęte są systemem dostępu za pomocą drzwi zamykanych na klucz, a budynek w którym znajduje się biuro objęty jest ochroną fizyczna.
2) Pomieszczenia, w których przetwarzane są zbiory danych osobowych zabezpieczone są przed skutkami pożaru za pomocą wolnostojącej gaśnicy.

Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej

1) Dostęp do systemu operacyjnego komputera, oraz do zewnętrznych narzędzi informatycznych w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
2) Zastosowano środki ochrony przed szkodliwym oprogramowaniem.
3) Wdrożono zasady wykonywania kopii zapasowych na systemach informatycznych.

Środki ochrony w ramach narzędzi programowych i baz danych

1) Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
2) Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.

Wprowadzanie zasad i procedur

Polityka bezpieczeństwa danych osobowych daje podstawę do opracowania i wdrożenia innych procedur ochrony danych osobowych.