POLITYKA PRZETWARZANIA

I OCHRONY DANYCH OSOBOWYCH

OBOWIĄZUJĄCA U:

1. **MAŁGORZATY NABIT PROWADZĄCEJ DZIAŁALNOŚĆ GOSPODARCZĄ POD NAZWĄ "TADEK" S.C. T. RASIŃSKI, I. NABIT, M. NABIT MAŁGORZATA NABIT WSPÓLNIK SPÓŁKI CYWILNEJ,**
2. **IRENEUSZA NABIT PROWADZĄCEGO DZIAŁALNOŚĆ GOSPODARCZĄ POD NAZWĄ "TADEK" S.C. T. RASIŃSKI, I. NABIT, M. NABIT IRENEUSZ NABIT WSPÓLNIK SPÓŁKI CYWILNEJ,**
3. **TADEUSZA RASIŃSKIEGO PROWADZĄCEGO DZIAŁALNOŚĆ GOSPODARCZĄ POD NAZWĄ "TADEK" S.C. T. RASIŃSKI, I. NABIT, M. NABIT TADEUSZ RASIŃSKI WSPÓLNIK SPÓŁKI CYWILNEJ**

DZIAŁAJĄCY WSPÓLNIE W RAMACH SPÓŁKI CYWILNEJ POD NAZWĄ:

TADEK SPÓŁKA CYWILNA T. RASIŃSKI, I. NABIT, M. NABIT

Z GŁÓWNYM MIEJSCEM WYKONYWANIA DZIAŁALNOŚCI GOSPODARCZEJ W MIEJSCOWOŚCI MOKRE

Obowiązuje od dnia 01.03.2025 r.

1. Cel dokumentu

1.1 Niniejszy dokument (zwany dalej „**Polityką**”) określa całość zasad przetwarzania i ochrony danych osobowych obowiązujących u:

a) Małgorzaty Nabit, prowadzącej działalność gospodarczą pod nazwą "TADEK" S.C. T. Rasiński, I. Nabit, M. Nabit Małgorzata Nabit wspólnik spółki cywilnej, NIP: 1251188869,

b) Ireneusza Nabit prowadzącego działalność gospodarczą pod nazwą "TADEK" S.C. T. Rasiński, I. Nabit, M. Nabit Ireneusz Nabit wspólnik spółki cywilnej, NIP: 9461664056,

c) Tadeusza Rasińskiego prowadzącego działalność gospodarczą pod nazwą "TADEK" S.C. T. Rasiński, I. Nabit, M. Nabit Tadeusz Rasiński wspólnik spółki cywilnej, NIP: 7161645875,

- działający wspólnie w ramach spółki cywilnej pod nazwą: **Tadek spółka cywilna T. Rasiński, I. Nabit, M. Nabit,** NIP: 1251463608, z głównym miejscem wykonywania działalności w miejscowości Mokre, zwani dalej łącznie „**Współadministratorami**” lub każdy z osobna „**Administratorem**”.

1.2 Dokument zawiera także wzory dokumentów stosowanych przez Współadministratorów w związku z przetwarzaniem danych osobowych.

1.3 Polityka i wdrożone zasady ochrony danych osobowych zostały opracowane z uwzględnieniem **przedmiotu działalności Współadministratorów, tj. działalności związanej z produkcją wyrobów cukierniczych.**

1.4 Zasady wdrożone w Polityce mają na celu zapewnienie najwyższej ochrony danych osobowych przetwarzanych przez Współadministratorów, z uwzględnieniem postanowień 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 („**RODO**”).

1.5 Polityka podlega aktualizacji wraz ze zmieniającymi się przepisami prawnymi oraz zmianami zachodzącymi u Współadministratorów, dotyczącymi przeprowadzanych operacji na Danych Osobowych. Przegląd przeprowadzany jest przez Współadministratorów co najmniej raz do roku, chyba że konieczność częstszych aktualizacji spowodowana jest istotnymi zmianami w przepisach prawa lub planowaną zmianą działalności Współadministratora.

2. Zakres stosowania

2.1 Polityka obowiązuje wszystkich pracowników i współpracowników Współadministratorów oraz inne osoby mające dostęp do Danych Osobowych. Dodatkowo Współadministratorzy zapewniają stosowanie zasad wynikających z Polityki przez podmioty przetwarzające dane osobowe na ich zlecenie na zasadach określonych w punkcie 11.

3. Terminologia

Skróty użyte w Polityce:

DANE OSOBOWE – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; 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 PESEL, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

OSOBA UPOWAŻNIONA – osoba, której Współadministratorzy wydali upoważnienie do przetwarzania Danych Osobowych, w zakresie wskazanym w upoważnieniu.

PODMIOT DANYCH – osoba fizyczna, której Dane Osobowe są przetwarzane.

PRZETWARZANIE DANYCH OSOBOWYCH – operacja lub zestaw operacji wykonywanych na Danych Osobowych w sposób zautomatyzowany lub niezautomatyzowany, taki jak zbieranie, przechowywanie, modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

SYSTEM INFORMATYCZNY – zespół współpracujących ze sobą urządzeń, programów, procedur i narzędzi programowych zastosowanych w celu Przetwarzania Danych Osobowych.

SZCZEGÓLNE KATEGORIE DANYCH OSOBOWYCH - dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej (np. wizerunek twarzy lub dane daktyloskopijne), dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

UODO – Urząd Ochrony Danych Osobowych.

USTAWA – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, uzupełniająca postanowienia RODO.

4. Odpowiedzialność

4.1 Za zapoznanie pracowników i współpracowników z Polityką i innymi zasadami Przetwarzania Danych Osobowych odpowiedzialna jest Małgorzata Nabit.

4.2 Każdy pracownik i współpracownik Współadministratorów, w szczególności Osoby Upoważnione, ponoszą odpowiedzialność za przestrzeganie bezpieczeństwa Danych Osobowych, w szczególności opisanych w Polityce.

4.3 Niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, naruszenie obowiązków określonych w Polityce może być podstawą rozwiązania umowy o pracę lub umowy o współpracy z osobą, która dopuściła się zawinionego naruszenia tych zasad.

4.4 Naruszenie zasad określonych w Polityce może być potraktowane jako nienależyte wykonanie umów cywilnoprawnych, w szczególności gdy wykonawca w razie naruszenia zasad ochrony Danych Osobowych lub uzasadnionego podejrzenia takiego naruszenia nie poinformował o tym Administratora. Rozwiązanie umowy z wykonawcą nie wyklucza jego odpowiedzialności karnej.

5. Zasady podstawowe

5.1 Współadministratorzy podejmują wszelkie kroki mające na celu zapewnienie prawidłowego Przetwarzania Danych Osobowych oraz zapewnienie najwyższej ochrony Danych Osobowych. W tym celu zapewniają:

a) **zgodność z prawem, rzetelność i przejrzystość** Przetwarzania Danych Osobowych;

b) **minimalizację danych** – Dane Osobowe są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;

c) **prawidłowość** – Dane Osobowe są zgodne ze stanem faktycznym i w razie potrzeby uaktualniane;

d) **ograniczenie celu** – zbieranie Danych Osobowych w konkretnych, wyraźnych i prawnie uzasadnionych celach oraz nieprzetwarzania Danych Osobowych w sposób niezgodny z celami;

e) **integralność i poufność** — Dane Osobowe są przetwarzane za pomocą odpowiednich środków technicznych oraz organizacyjnych; w sposób gwarantujący odpowiednie zabezpieczenie Danych Osobowych, w tym ochronę przed niezgodnym z prawem przetwarzaniem oraz przypadkowym udostępnieniem;

f) **ograniczenie przechowywania** – Dane Osobowe są przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których Dane Osobowe są przetwarzane;

g) **rozliczalność** — Współadministratorzy są odpowiedzialni za przestrzeganie powyższych zasad, uwzględnienie ich na etapie projektowania (*privacy by design)* oraz wykazanie ich przestrzegania.

6. Rejestr czynności przetwarzania

6.1 Mając na względzie fakt, że przetwarzanie przez Administratorów danych nie ma charakteru sporadycznego, każdy z Administratorów prowadzi rejestr czynności przetwarzania, stanowiący odpowiednio **Załącznik nr 1a, Załącznik nr 1b oraz Załącznik nr 1c.** Rejestr czynności przetwarzania przechowywany jest w formacie elektronicznym excel i jest na bieżąco aktualizowany.

6.2 Współadministratorzy w ramach zainstalowanego systemu monitoringu wizyjnego, przetwarzają szczególne kategorie Danych Osobowych, to jest dane biometryczne w postaci wizerunku twarzy. Współadministratorzy mogą również przetwarzać szczególne Dane Osobowe zatrudnionych osób, obejmujące dane o stanie zdrowia, w zakresie dozwolonym przez przepisy prawa pracy, zabezpieczenia społecznego i ochrony socjalnej. Współadministratorzy nie przetwarzają innych szczególnych kategorii Danych Osobowych.

6.3 Przez szczególne kategorie Danych Osobowych rozumie się dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej (np. wizerunek twarzy lub dane daktyloskopijne), dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

7. Analiza ryzyka

7.1 Współadministratorzy dokonali analizy ryzyka Przetwarzania Danych Osobowych na podstawie kryteriów stanowiących **Załącznik nr 2** do Polityki oraz informacji zawartych w Polityce.

7.2 W wyniku oceny:

a) przeprowadzonej analizy ryzyka;
b) sporządzonego rejestru czynności przetwarzania;
c) zgodności przetwarzania danych osobowych z RODO;

Współadministratorzy uznali, że przeprowadzenie oceny skutków dla ochrony danych nie jest konieczne.

7.3 Współadministratorzy dokonują ponownej analizy ryzyka w przypadku zmiany kategorii przetwarzanych Danych Osobowych, zmiany procedur obowiązujących u Współadministratorów lub zmiany obowiązującego prawa.

8. Podział zadań

8.1 **Postanowienia ogólne**

8.1.3 Administratorzy są współadministratorami Danych Osobowych, czyli podmiotami odpowiedzialnymi za Przetwarzanie Danych Osobowych oraz za ich ochronę zgodnie z postanowieniami RODO, Ustawy i innych obowiązujących przepisów prawa.

8.1.4 Bez względu na powyższe, wszystkie Osoby Upoważnione są zobowiązane do zapewnienia bezpieczeństwa Przetwarzania Danych Osobowych.

8.2 **Inspektor Ochrony Danych**

8.2.1 Mając na względzie fakt, że nie zachodzą przesłanki wskazane w art. 37 ust. 1 RODO, Współadministratorzy nie powołują Inspektora Ochrony Danych. Analiza zasadności powołania Inspektora Ochrony Danych stanowi **Załącznik nr 3** do Polityki.

8.3 **Współadministrator Danych Osobowych**

8.3.1 Współadministratorami Danych Osobowych są: Małgorzata Nabit, prowadząca działalność gospodarczą pod nazwą "TADEK" S.C. T. Rasiński, I. Nabit, M. Nabit Małgorzata Nabit wspólnik spółki cywilnej, Ireneusz Nabit prowadzący działalność gospodarczą pod nazwą "TADEK" S.C. T. Rasiński, I. Nabit, M. Nabit Ireneusz Nabit wspólnik spółki cywilnej, Tadeusz Rasiński prowadzący działalność gospodarczą pod nazwą "TADEK" S.C. T. Rasiński, I. Nabit, M. Nabit Tadeusz Rasiński wspólnik spółki cywilnej, działający wspólnie w ramach spółki cywilnej pod nazwą: Tadek spółka cywilna T. Rasiński, I. Nabit, M. Nabit z głównym miejscem wykonywania działalności w miejscowości Mokre.

8.3.2 Adres Współadministratorów: ul. 15-go Sierpnia nr 35, 05-250 Mokre.

8.3.3 Dane kontaktowe Współadministratorów:
Adres korespondencyjny: ul. 15-go Sierpnia nr 35, 05-250 Mokre.
e-mail: biuro@ciastadomowe.eu

8.3.4 Obowiązki Współadministratorów wykonuje Małgorzata Nabit.

8.3.5 Do podstawowych obowiązków Współadministratorów należy:

a) identyfikacja obszarów, w których są przetwarzane Dane Osobowe;
b) identyfikacja kategorii Danych Osobowych z uwzględnieniem zasady minimalizacji Danych Osobowych;
c) nadzór nad prawidłowym Przetwarzaniem Danych Osobowych, w tym decydowanie o nadaniu upoważnień z uwzględnieniem zasady minimalizacji Danych Osobowych;
d) zapewnienie prawidłowości przetwarzania oraz skutecznej ochrony Danych Osobowych zgodnie z zasadami wynikającymi z RODO;
e) podział zadań i obowiązków związanych z ochroną Danych Osobowych;
f) implementacja i aktualizacja środków technicznych i organizacyjnych zapewniających prawidłowe Przetwarzanie Danych Osobowych oraz możliwość wykazania prawidłowości Przetwarzania Danych Osobowych;
g) zapewnienie okresowych przeglądów Przetwarzania Danych Osobowych, analizy ryzyka oraz obowiązującej Polityki.

8.4 **Osoby upoważnione**

8.4.1 Do przetwarzania Danych Osobowych dopuszczane są jedynie osoby posiadające upoważnienie do przetwarzania danych osobowych.

8.4.2 Nadawaniem uprawnień do przetwarzania Danych Osobowych zajmuje się Małgorzata Nabit.

8.4.3 Dostęp do Danych Osobowych jest przyznawany tylko takim osobom, dla których dostęp jest niezbędny do wykonania ich obowiązków lub zapewnienia ochrony Danych Osobowych.

8.4.4 Upoważnienia są wydawane przed rozpoczęciem Przetwarzania Danych Osobowych po dostarczeniu Współadministratorom podpisanego Oświadczenia, którego wzór stanowi **Załącznik nr 4** do niniejszej Polityki.

8.4.5 Upoważnienie sporządzane jest zgodnie ze wzorem stanowiącym **Załącznik nr 5** do Polityki.

8.4.6 Ewidencja Osób Upoważnionych do Przetwarzania Danych Osobowych jest prowadzona przez Współadministratorów zgodnie ze wzorem stanowiącym **Załącznik nr 6**.

8.4.7 Osoba Upoważniona zobowiązana jest do znajomości obowiązujących zasad ochrony Danych Osobowych, w tym niniejszej Polityki i powinna stosować w możliwie najszerszym zakresie wszelkie dostępne środki tej ochrony, co w szczególności dotyczy uniemożliwienia osobom nieuprawnionym dostępu do Przetwarzanych Danych Osobowych.

8.4.8 Osoby Upoważnione do przetwarzania Danych Osobowych przechodzą okresowe szkolenia dotyczące obowiązujących u Współadministratorów zasad przetwarzania i ochrony Danych Osobowych.

8.4.9 Do obowiązków Osoby Upoważnionej należy także:

a) przetwarzanie Danych Osobowych zgodnie z obowiązującymi przepisami prawa oraz obowiązującą Polityką i innymi wewnętrznymi regulacjami;
b) zachowanie w tajemnicy Danych Osobowych oraz informacji o sposobach ich zabezpieczenia;
c) niezwłoczne informowanie Współadministratorów o wszelkich podejrzeniach incydentów związanych z naruszeniem zasad Przetwarzania Danych.

9. Realizacja uprawnień podmiotu danych

9.1 Podstawowe zasady

9.1.1 Podmiot Danych jest uprawniony do:

a) otrzymania informacji o danych Współadministratorów, zasadach przetwarzania danych oraz przysługujących mu uprawnieniach, na zasadach określonych w pkt 9.2 poniżej;
b) uzyskania potwierdzenia, czy przetwarzane są dane, które go dotyczą, a jeżeli ma to miejsce – uzyskania dostępu oraz otrzymania informacji, o których mowa w pkt 9.3 poniżej (prawo dostępu);
c) żądania niezwłocznego sprostowania dotyczących go Danych Osobowych, które są nieprawidłowe oraz (z uwzględnieniem celów przetwarzania) żądania uzupełniania niekompletnych danych Osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia;
d) żądania niezwłocznego usunięcia dotyczących go Danych Osobowych (prawo do bycia zapomnianym);
e) żądania ograniczenia przetwarzania Danych Osobowych;
f) przenoszenia Danych Osobowych;
g) wniesienia sprzeciwu wobec przetwarzania dotyczących go Danych Osobowych;

9.1.2 Działania, o których mowa w pkt 9.1.1 lit. b) -g), podejmowane są na wniosek Podmiotu Danych.

9.1.3 Wnioski powinny być kierowane na adres e-mail: biuro@ciastadomowe.eu lub na adres: ul. 15-go Sierpnia nr 35, 05-250 Mokre.

9.1.4 Wnioski, o których mowa w pkt 9.1.3, rozpatrywane są przez Małgorzatę Nabit.

9.1.5 Jeżeli wniosek budzi wątpliwości osoby go rozpatrującej, w tym co do zakresu żądanych informacji, osoba ta może zwrócić się do Podmiotu Danych z prośbą o wyjaśnienie niejasności.

9.1.6 Odpowiedzi na wnioski, o których mowa w pkt 9.1.1 lit. b) -f) udziela się pisemnie w terminie miesiąca od otrzymania wniosku, chyba że Podmiot Danych wskazał inną formę.

9.1.7 Termin, o którym mowa w pkt 9.1.6 może być przedłużony o dwa miesiące ze względu na skomplikowany charakter żądania lub liczbę żądań. Osoba rozpatrująca wniosek jest zobowiązana do poinformowania Podmiotu Danych o przedłużeniu terminu oraz jego przyczynach.

9.1.8 Działania, o których mowa w niniejszym rozdziale, podejmowane są bezpłatnie. Jeżeli żądania są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, Współadministratorzy mogą zadecydować o:

a) odmowie podjęcia działań;
b) pobraniu opłaty, która nie może być wyższa niż koszty faktycznie poniesione przez Współadministratorów w związku z rozpatrywaniem wniosku.

9.1.9 Osoba rozpatrująca wniosek jest upoważniona do dokonania weryfikacji tożsamości Podmiotu Danych, o ile zachodzą co do tego wątpliwości, poprzez wgląd do dowodu osobistego lub innego dokumentu tożsamości.

9.1.10 Współadministratorzy w terminie 14 dni informują o sprostowaniu lub usunięciu Danych Osobowych lub ograniczeniu ich przetwarzania zgodnie z wnioskiem, każdego odbiorcę, któremu ujawniono Dane Osobowe, chyba że będzie to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

9.2 **Informacja udzielana Podmiotowi Danych**

9.2.1 Podmiot Danych przed rozpoczęciem Przetwarzania Danych Osobowych otrzymuje od Współadministratorów na piśmie następujące informacje:

a) dane Współadministratorów;
b) cel i podstawę prawną Przetwarzania Danych Osobowych;
c) okres, przez który Dane Osobowe są przetwarzane lub kryteria ustalenia tego okresu;
d) prawo dostępu do Danych Osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz prawo wniesienia sprzeciwu wobec ich przetwarzania;
e) prawo do cofnięcia zgody w dowolnym momencie (jeżeli przetwarzanie danych odbywa się na podstawie zgody);
f) prawo do wniesienia skargi do organu nadzorczego;
g) kategorie odbiorców Danych Osobowych;
h) informację, czy podanie danych jest wymogiem ustawowym czy umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych.

9.2.2 Informacji, o których mowa w pkt. 9.2.1, nie udziela się, jeżeli Podmiot Danych dysponuje już tymi danymi.

9.2.3 Informacje, o których mowa w pkt 9.2.1 zawarte są w klauzulach informacyjnych, znajdujących się w folderze „Klauzule". Klauzule informacyjne są udostępniane Podmiotom Danych w następujący sposób:

a) Pracownikom i Współpracownikom – jako załącznik do umowy;
b) Kandydatom do pracy – pierwsza warstwa w ogłoszeniu o pracę, pozostałe informacje są udostępniane podczas pierwszego kontaktu z kandydatem;
c) Klientom/Partnerom biznesowym Współadministratorów oraz zainteresowanym współpracą ze Współadministratorami - poprzez odesłanie do klauzul na stronie internetowej Współdministratorów lub jako załącznik do umowy;

d) Innym osobom – poprzez odesłanie do klauzuli na stronie internetowej Współadministratorów.

9.3 **Prawo dostępu przysługujące Podmiotowi Danych**

9.3.1 Podmiot Danych może uzyskać od Współadministratorów potwierdzenie, czy jego Dane Osobowe są przetwarzane, a jeżeli tak, jest uprawniony do uzyskania dostępu do nich oraz uzyskania informacji o:

a) celach przetwarzania;
b) źródle danych (jeżeli nie zostały zebrane bezpośrednio od Podmiotu Danych);
c) kategoriach przetwarzanych Danych Osobowych;
d) odbiorcach lub kategoriach odbiorców, którym Dane Osobowe zostały lub zostaną ujawnione;
e) planowanym okresie przechowywania Danych Osobowych, a gdy nie jest to możliwe – o kryteriach ustalania tego okresu;
f) przysługujących mu prawach.

9.3.2 Wraz z informacją, o której mowa powyżej, Podmiotowi Danych dostarcza się kopię Danych Osobowych podlegających przetwarzaniu. Kopia przekazywana jest w formie e-mail, chyba że Podmiot Danych wskazał inną formę.

9.3.3 Za wszelkie kolejne kopie, o które zwróci się Podmiot Danych w przeciągu dwóch miesięcy od otrzymania poprzedniej kopii, Współadministratorzy pobierają opłatę w wysokości odpowiadającej kosztom administracyjnym poniesionym przez Współadministratorów w związku ze sporządzeniem takiej kopii.

10. Bezpieczeństwo przetwarzania danych osobowych

10.1 Osoby Upoważnione mają obowiązek podejmowania działań w celu zapewnienia najwyższej ochrony Danych Osobowych.

10.2 Współadministratorzy ustalają następujące podstawowe zasady bezpieczeństwa:

a) Dostęp do danych osobowych jest przyznawany na zasadzie minimalizacji: podmioty uprawnione otrzymują dostęp tylko do tych danych, które są im niezbędne do wykonywania swoich obowiązków, wg zasad:
   i. Dostęp na podstawie ról: Każdy podmiot w organizacji ma przypisaną rolę, a dostęp do danych jest ograniczony do zakresu obowiązków wynikających z tej roli.
   ii. Zasada „need-to-know”: Dostęp do danych wrażliwych (jeśli są zbierane) jest udzielany wyłącznie podmiotom, które mają wyraźną potrzebę ich przetwarzania w ramach swoich obowiązków.
   iii. Zasada minimalizacji dostępu: Dane osobowe są udostępniane tylko w takim zakresie, w jakim jest to niezbędne do realizacji celu przetwarzania.
   iv. Przyznawanie dostępu jest dokonywane przez upoważnione osoby (np. administratora systemów), na podstawie analizy potrzeb danego podmiotu. Po przyznaniu dostępu, użytkownik jest regularnie weryfikowany pod kątem zgodności z wymaganiami dostępu.
b) Wszystkie systemy, aplikacje oraz bazy danych przetwarzające dane osobowe w organizacji są zabezpieczone mechanizmami autoryzacji, które pozwalają na przyznawanie dostępu do tych zasobów jedynie upoważnionym użytkownikom. Każdy użytkownik systemu otrzymuje dostęp na podstawie roli i zakresu obowiązków służbowych.
c) W celu zapewnienia bezpieczeństwa procesów uwierzytelniania stosowane są następujące metody:

i. Stosowanie haseł do komputerów. Użytkownicy są zobowiązani do stosowania haseł o minimalnej długości 12 znaków, zawierających małe i wielkie litery, cyfry oraz znaki specjalne.
ii. Na komputerach używane są konta Microsoft. Wymagają one odpowiednio złożonego hasła zmienianego okresowo;
iii. Stosowanie pinów do smartfonów;
iv. Autentykacja wieloskładnikowa.

d) Stosowanie wygaszaczy ekranów w komputerach;
e) Zabezpieczenia serwerów;
f) Szyfrowanie danych – wykorzystywane do ochrony danych przechowywanych i przesyłanych, zapewniając, że tylko upoważnione osoby mogą je odczytać;
g) Szafy z dokumentami zamykane na klucz;
h) Ochrona budynku;
i) Dostęp do pomieszczeń przedsiębiorstwa jedynie przy użyciu klucza/karty dostępu;
j) Niszczenie niepotrzebnych dokumentów;
k) Zasada ograniczonego dostępu do danych, upoważnienia nadawane są zgodnie z zakresem obowiązków;
l) Regularne kopie zapasowe;
m) Ochrona przed złośliwym oprogramowaniem;
n) Fizyczne zabezpieczenia serwerowni – ograniczony i monitorowany dostęp do sprzętu- tylko dla autoryzowanego personelu;
o) Stosowanie ochrony przed atakami typu DDoS oraz dodatkowych warstw bezpieczeństwa;
p) Stosowanie zapór sieciowych (Firewalls);
q) Regularne aktualizacje oprogramowania;
r) Praca wyłącznie na sprzęcie służbowym (telefony, komputery);
s) stosowanie monitoringu pomieszczeń przedsiębiorstwa;
t) Dostęp do danych przetwarzanych w systemach informatycznych i na serwerach jest możliwy tylko po uwierzytelnieniu;
u) Każda osoba mająca dostęp do danych zostaje zapoznana z zasadami ochrony Danych;
v) Osoby mające dostęp do Danych Osobowych zobowiązane są do zachowania Danych Osobowych oraz informacji o sposobach ich zabezpieczenia w tajemnicy;
w) Zobowiązanie do zachowania w tajemnicy Danych Osobowych oraz sposobów ich zabezpieczenia odbywa się także za pośrednictwem odbieranych pisemnych oświadczeń od osób dopuszczonych do przetwarzania Danych Osobowych.

10.3. Współadministratorzy przeprowadzają regularne audyty wewnętrzne, mające na celu identyfikację ewentualnych luk w zabezpieczeniach.

11. Udostępnianie i powierzanie przetwarzania danych osobowych

11.1 Udostępnianie danych osobowych

11.1.1 Dane Osobowe mogą być udostępniane wyłącznie podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa oraz Podmiotom Danych.

11.1.2 Zasady udostępniania Danych Osobowych Podmiotom Danych wskazane są w punkcie 9.

11.1.3 Udostępnianie Danych Osobowych następuje wyłącznie z uwzględnieniem zasad ich bezpieczeństwa, w tym zasady minimalizacji danych.

11.1.4 Informacje zawierające Dane Osobowe powinny być przekazywane uprawnionym podmiotom w sposób gwarantujący ochronę Danych Osobowych.

11.1.5 Udostępniając Dane Osobowe innym podmiotom, Współadministratorzy mają obowiązek odnotowywać informacje o udostępnieniu, w tym: informacje o odbiorcy Danych Osobowych, datę i zakres udostępnionych Danych Osobowych, podstawę prawną udostępnienia.

11.1.6 Udostępniając Dane Osobowe, należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

11.2 Powierzanie przetwarzania danych osobowych

11.2.1 Współadministratorzy powierzają przetwarzanie Danych Osobowych przede wszystkim podmiotom, które na ich zlecenie świadczą usługi np. księgowe, marketingowe i inne.

11.2.2 Powierzenie Przetwarzania Danych Osobowych następuje wyłącznie na podstawie pisemnej umowy, która określa w szczególności:

a) rodzaj Danych Osobowych;
b) kategorie osób, których dane dotyczą;
c) okres na jaki dane są powierzone;
d) obowiązki i prawa Współadministratorów;
e) zakres odpowiedzialności podmiotu, któremu powierzono przetwarzanie danych, z tytułu niewykonania lub nienależytego wykonania umowy;
f) zobowiązanie podmiotu zewnętrznego do Przetwarzania Danych Osobowych wyłącznie na udokumentowane polecenie Współadministratorów.

11.2.3 Powierzenie Przetwarzania Danych Osobowych musi uwzględniać wymogi określone w art. 28 RODO. W szczególności podmiot zewnętrzny, któremu ma zostać powierzone Przetwarzanie Danych Osobowych, jest obowiązany przed rozpoczęciem Przetwarzania Danych Osobowych do podjęcia środków wymaganych na mocy art. 32 RODO.

11.2.4 Podmiot Przetwarzający Dane Osobowe nie może podzlecać przetwarzania Danych Osobowych bez uzyskania uprzedniej pisemnej zgody Współadministratorów.

11.2.5 Powierzenie Przetwarzania Danych Osobowych nie oznacza zwolnienia Współadministratorów z odpowiedzialności za zgodne z prawem Przetwarzanie Danych Osobowych, co oznacza konieczność zapewnienia Współadministratorom uprawnienia do przeprowadzenia w siedzibie podmiotu zewnętrznego kontroli wykonania umowy stanowiącej podstawę powierzenia Przetwarzania Danych Osobowych m. in. w zakresie obowiązujących regulacji wewnętrznych, udzielonych Upoważnień do przetwarzania danych oraz zobowiązań do zachowania tajemnicy. Podmiot zewnętrzny powinien także udostępnić Współadministratorom wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w RODO.

12. Zarządzanie incydentami

12.1 Zdarzenia naruszające bezpieczeństwo danych osobowych

12.1.1 Zagrożenia losowe naruszające bezpieczeństwo Danych Osobowych są to:

a) zagrożenia losowe wewnętrzne (np. pomyłki, błędy oprogramowania, awarie sprzętu);
b) zagrożenia losowe zewnętrzne (np. przerwy w dostawie prądu, klęski żywiołowe,).

12.1.2 Zagrożenia mogą być również celowe, do których zalicza się:

a) nieuprawniony dostęp do Systemu Informatycznego z zewnątrz (włamanie),
b) nieuprawniony dostęp do Systemu Informatycznego spowodowany przez pracownika,
c) nieuprawnione udostępnienie Danych Osobowych,
d) pogorszenie jakości Systemu Informatycznego skutkujące utratą lub obniżeniem poziomu ochrony poufności.

12.1.3 Naruszeniem bezpieczeństwa Danych Osobowych jest także nieprawidłowe zabezpieczenie miejsc przechowywania Danych Osobowych, w tym dostęp do komputerów dla osób nieupoważnionych, otwarte szafy z aktami, pozostawienie nośników w miejscu publicznym.

12.2 **Monitorowanie i zgłaszanie incydentów**

12.2.1 Każda osoba, która zauważyła zdarzenie mogące spowodować naruszenie bezpieczeństwa Danych Osobowych zobowiązana jest do natychmiastowego poinformowania Małgorzaty Nabit.

12.2.2 Po otrzymaniu zgłoszenia o możliwości naruszenia bezpieczeństwa Danych Osobowych Małgorzata Nabit bezzwłocznie podejmuje działania mające na celu:

a) wyjaśnienia zdarzenia, w tym stwierdzenie czy miało miejsce naruszenie bezpieczeństwa Danych Osobowych – w tym celu wypełnia się formularz Analizy pod kątem ryzyka naruszenia praw i wolności osób fizycznych, niezbędnej do oceny, czy doszło do naruszenia ochrony danych osobowych powodującego konieczność zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych oraz osób, których dotyczy naruszenie;
b) wyjaśnienia przyczyn naruszenia i zebrania ewentualnych dowodów naruszenia zasad ochrony Danych Osobowych,
c) minimalizację skutków naruszenia Danych Osobowych,
d) usunięcie skutków incydentu.

12.2.3 Wyjaśnienie zgłoszonego zdarzenia następuje w szczególności poprzez:

a) przeprowadzenie analizy poprawności funkcjonowania systemu informatycznego,
b) weryfikację sposobów zabezpieczenia przetwarzania danych w systemie informatycznym, w szczególności danych konfiguracyjnych tego systemu informatycznego.

12.2.4 Po wyjaśnieniu incydentu związanego z bezpieczeństwem Danych Osobowych, Małgorzata Nabit, sporządza raport, który zawiera między innymi:

a) Opis zidentyfikowanego incydentu;
b) Podjęte działania mające na celu zminimalizowanie skutków incydentu;
c) Ewentualne działania mające na celu zapobieżenie wystąpienia takiego incydentu w przyszłości;
d) Analizę pod kątem ryzyka naruszenia praw lub wolności osób fizycznych, niezbędną do oceny czy doszło do naruszenia ochrony danych – w postaci załączonego wypełnionego formularza;

12.2.5 Raporty z incydentów archiwizuje się u Współadministratorów do celów dowodowych. Wzór raportu z incydentu stanowi **Załącznik nr 7** do Polityki.

12.2.6 Współadministratorzy prowadzą ewidencję interwencji związanych z zaistniałymi incydentami w zakresie bezpieczeństwa Danych Osobowych zawierającą następujące informacje:

a) imię i nazwisko zgłaszającego incydent,
b) imię i nazwisko osoby przyjmującej zgłoszenie incydentu,
c) datę zgłoszenia incydentu,
d) okoliczności naruszenia Ochrony Danych Osobowych,
e) skutki naruszenia Ochrony Danych Osobowych,
f) przeprowadzone działania wyjaśniające przyczyny zaistnienia incydentu,
g) wyniki przeprowadzonych działań,
h) podjęte akcje naprawcze i ocena ich skuteczności.

12.2.7 Ewidencja interwencji stanowi **Załącznik nr 8** do Polityki. Ewidencja interwencji prowadzona jest w wersji papierowej lub w wersji elektronicznej.

12.2.8 Co najmniej raz do roku Współadministratorzy przeprowadzają analizę zaistniałych incydentów w celu:

a) określenia skuteczności podejmowanych działań wyjaśniających i naprawczych,

b) określenia wymaganych działań zwiększających bezpieczeństwo Systemu Informatycznego i minimalizujących ryzyko zaistnienia incydentów,

c) określenia potrzeb w zakresie szkoleń Osób Upoważnionych.

12.3 **Zgłaszanie naruszeń do UODO**

12.3.1 W przypadku naruszenia bezpieczeństwa Danych Osobowych Współadministratorzy nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, zgłaszają je do UODO.

12.3.2 Zgłoszenia nie dokonuje się, jeżeli, w oparciu o raport z incydentu i przeprowadzoną analizę ryzyka pod kątem naruszenia praw lub wolności osób fizycznych niezbędną do oceny czy doszło do naruszenia ochrony danych, Współadministratorzy stwierdzą, że do naruszenia nie doszło, lub jest mało prawdopodobne by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

12.3.3 Jeżeli zgłoszenie jest dokonane po upływie 72 godzin od stwierdzenia naruszenia, do zgłoszenia załącza się wyjaśnienie przyczyn opóźnienia.

12.3.4 Współadministratorzy dokonuje powiadomienia za pomocą formularza dostępnego w serwisie UODO.

13. Postanowienia końcowe

13.1 Następujące załączniki do Polityki stanowią jej integralną część:

13.1.1 Załącznik nr 1a - rejestr czynności przetwarzania - Małgorzata Nabit, prowadząca działalność gospodarczą pod nazwą "TADEK" S.C. T. Rasiński, I. Nabit, M. Nabit Małgorzata Nabit wspólnik spółki cywilnej;

13.1.2 Załącznik nr 1b - rejestr czynności przetwarzania - Ireneusz Nabit, prowadzący działalność gospodarczą pod nazwą "TADEK" S.C. T. Rasiński, I. Nabit, M. Nabit Ireneusz Nabit wspólnik spółki cywilnej;

13.1.3 Załącznik nr 1c - rejestr czynności przetwarzania – Tadeusz Rasiński, prowadzący działalność gospodarczą pod nazwą "TADEK" S.C. T. Rasiński, I. Nabit, M. Nabit Tadeusz Rasiński wspólnik spółki cywilnej;

13.1.4 Załącznik nr 2 - kryteria dokonywania analizy ryzyka;

13.1.5 Załącznik nr 3 – analiza zasadności powołania IOD;

13.1.6 Załącznik nr 4 - oświadczenie o przestrzeganiu przepisów o ochronie Danych Osobowych;

13.1.7 Załącznik nr 5 - upoważnienie do Przetwarzania Danych Osobowych - wzór;

13.1.8 Załącznik nr 6 - ewidencja Osób Upoważnionych - wzór;

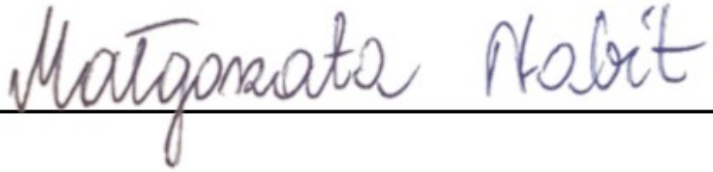
13.1.9 Załącznik nr 7 – wzór raportu z incydentu;

13.1.10 Załącznik nr 8 - ewidencja interwencji;

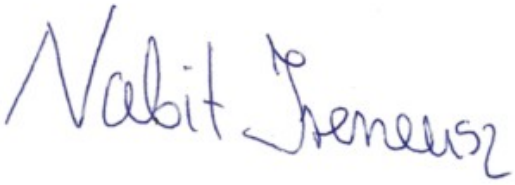
13.2 W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy RODO, Ustawy oraz przepisy wykonawcze do Ustawy.

13.3 Niniejsza Polityka wchodzi w życie z dniem przyjęcia.

Podpisy Współadministratorów:



Małgorzata Nabit



Ireneusz Nabit

Tadeusz Rasiński