knowit

POLITYKA
OCHRONY DANYCH OSOBOWYCH
W KNOWIT POLAND SP. Z O.O.

10 lutego 2022 r.

Knowit Poland sp. z o.o.
ul. Hrubieszowska 2
01-209 Warszawa
NIP: 951 178 99 96

Ph +48 22 355 21 70
Fax +48 22 355 21 71
www.knowit.eu

KRS 0000036076
Sąd Rejonowy dla m.st. Warszawy
XII Wydział Gospodarczy KRS
Kapitał zakładowy: 1 251 200 PLN

knowit

POLITYKA OCHRONY DANYCH OSOBOWYCH
W KNOWIT POLAND SP. Z O.O.

1. DEFINICJE

Na potrzeby Polityki Ochrony Danych Osobowych przyjmuje się następujące definicje:

(1) „**Administrator**" – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;

(2) „**Knowit PL**" – Knowit Poland sp. z o.o. z siedzibą w Warszawie, ul. Hrubieszowska 2, 01-209 Warszawa, wpisana do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m. st. Warszawy w Warszawie XII Wydział Gospodarczy pod numerem KRS: 0000036076, NIP: 951-17-89-996; REGON: 01284093700000, kapitał zakładowy: 1.251.200,00 zł;

(3) „**Dane Osobowe**" – oznaczają 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, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

(4) „**Koordynator Ochrony Danych Osobowych**", „**KODO**" lub "**Data Protection Coordinator**"– ustanowiona w Knowit PL funkcja niezależnego eksperta z zakresu ochrony Danych Osobowych nadzorującego przetwarzanie Danych Osobowych w Knowit PL;

(5) „**Naruszenie**" – 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;

(6) „**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 Europejskiej 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;

(7) „**Organ Nadzorczy**" – oznacza niezależny organ publiczny odpowiedzialny za monitorowanie stosowania przepisów o ochronie Danych Osobowych, ustanowiony przez państwo członkowskie Unii Europejskiej zgodnie z art. 51 RODO;

(8) „**Personel**" – oznacza Pracowników i Współpracowników Knowit PL;

(9) „**Podmiot Przetwarzający**" – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza Dane Osobowe w imieniu Administratora;

(10) „**Polityka Ochrony Danych Osobowych**" lub "**POD**" – oznacza niniejszy dokument wraz z Załącznikami;

(11) „**Prezes Urzędu Ochrony Danych Osobowych**" lub „**PUODO**" – oznacza ustanowiony w Polsce Organ Nadzorczy;

(12) „**Pracownik**" – oznacza osobę związaną stosunkiem pracy z Knowit PL;

(13) „**Procedura Obsługi Naruszeń**" lub „**PON**" – oznacza procedurę postępowania w przypadku naruszenia ochrony Danych Osobowych obowiązującą w Knowit PL;

(14) „**Procedura Obsługi Żądań**" lub „**POŻ**" – oznacza procedurę postępowania w przypadku zgłoszenia Żądania przez osobę, której dane dotyczą obowiązującą w Knowit PL;

(15) „**Przetwarzanie**" – 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;

(16) „**Rejestr Naruszeń Danych Osobowych**" – oznacza rejestr stwierdzonych w Knowit PL przypadków naruszenia ochrony Danych Osobowych;

(17) „**Rejestr Żądań**" – oznacza rejestr zgłoszonych do Knowit PL żądań dotyczących uprawnień osób fizycznych, o których mowa w art 15-22 RODO;

(18) „**RODO**" – oznacza 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 (ogólne rozporządzenie o ochronie danych) (Dz.U. UE. L. z 2016 r. Nr 119, str. 1);

(19) „**Współpracownik**" – oznacza osobę związaną z Knowit PL stosunkiem zlecenia lub innej umowy cywilnoprawnej, a także praktykanta i stażystę;

(20) „**Zawiadomienie PD**" – oznacza dopełnienie obowiązku wynikającego z Procedury Obsługi Naruszeń oraz przepisów prawa w razie stwierdzenia Naruszenia przez zawiadomienie podmiotu danych, którego dotyczy Naruszenie (osoby, której dane dotyczą), o takim Naruszeniu;

(21) „**Zawiadomienie PUODO**" – oznacza dopełnienie obowiązku wynikającego z Procedury Obsługi Naruszeń oraz przepisów prawa przez złożenie zawiadomienia do Prezesa Urzędu Ochrony Danych Osobowych o stwierdzeniu Naruszenia.

(22) „**Zgoda**" – 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.

2. CEL I ZAKRES POLITYKI

1. W celu zapewnienia ochrony Danych Osobowych w Knowit PL oraz dostosowania działalności do wymagań RODO, a także dalszych przepisów krajowych o ochronie Danych Osobowych, przyjmuje się do stosowania w Knowit PL Politykę Ochrony Danych Osobowych.

2. Polityka Ochrony Danych Osobowych reguluje:
   (1) zasady postępowania z Danymi Osobowymi w Knowit PL,
   (2) zasady prowadzenia dokumentacji związanej z przetwarzaniem Danych Osobowych,
   (3) sposób postępowania z Żądaniami osób, których dane dotyczą;
   (4) sposób postępowania z Naruszeniami;
   (5) zasady dotyczące oceny działalności dla praw i wolności osób, których dane dotyczą;
   (6) zasady związane z zapewnieniem bezpieczeństwa Danych Osobowych;
   (7) tryb zawierania umów powierzenia przetwarzania z klientami i dostawcami.
3. Integralną częścią Polityki Ochrony Danych Osobowych są następujące Załączniki:
   (1) Procedura Obsługi Żądań osób, których dane dotyczą;
   (2) Procedura Obsługi Naruszeń.

3. OCHRONA DANYCH OSOBOWYCH W KNOWIT PL – ZASADY OGÓLNE

1. **Podstawy postępowania z Danymi Osobowymi**. Sposób postępowania w Knowit PL z Danymi Osobowymi opiera się na czterech podstawach:
   a) legalność – Knowit PL dba o ochronę prywatności i przetwarza Dane Osobowe zgodnie z prawem;
   b) bezpieczeństwo – Knowit PL zapewnia odpowiedni poziom bezpieczeństwa Danych Osobowych, podejmując stale działania w tym zakresie;
   c) poszanowanie praw jednostki – Knowit PL umożliwia osobom, których dane przetwarza, wykonywanie ich praw i prawa te realizuje;
   d) rozliczalność – Knowit PL dokumentuje sposób wypełnienia obowiązków związanych z ochroną Danych Osobowych, aby w każdej chwili móc wykazać zgodność z obowiązującymi przepisami prawa.
2. **Zasady ochrony Danych Osobowych w Knowit PL**. Knowit PL przetwarza Dane Osobowe z poszanowaniem następujących zasad:
   a) zgodnie z prawem i rzetelnie (zgodność z prawem i rzetelność);
   b) w sposób przejrzysty dla osoby, której dane dotyczą (przejrzystość);
   c) w konkretnych, wyraźnych i prawnie uzasadnionych celach (ograniczenie celu);
   d) w zakresie adekwatnym i niezbędnym do realizacji celu (adekwatność i minimalizacja);
   e) z dbałością o prawidłowość danych (prawidłowość);
   f) nie dłużej niż jest to niezbędne do celów, w których dane są przetwarzane (ograniczenie przechowywania);
   g) zapewniając odpowiednie bezpieczeństwo danych w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych i organizacyjnych (bezpieczeństwo).
3. **System ochrony Danych Osobowych**. W Knowit PL obowiązuje system ochrony Danych Osobowych, który składa się z następujących elementów:

Projektowanie prywatności (*Privacy by design*) – Knowit PL zapewnia, aby w każdym obszarze prowadzonej działalności uwzględniane były zasady dotyczące ochrony prywatności i przetwarzania Danych Osobowych. W tym celu stale kontroluje i, w miarę zidentyfikowanych potrzeb, modyfikuje procedury dotyczące istniejących procesów. W przypadku uruchamiania nowych projektów i inwestycji w Knowit PL, dokonywana jest oceny wpływu zmiany na ochronę Danych Osobowych, analizę ryzyka, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji lub na początku nowego projektu. Zasada *privacy by design* realizowana jest przez zapewnienie audytów istniejących procesów oraz udziału KODO w pracach dotyczących nowego projektu lub planowanej inwestycji.

Minimalizacja (*Privacy by default*) – Knowit PL posiada zasady i metody zarządzania minimalizacją, obejmujące dostosowanie zakresu i liczby przetwarzanych Danych Osobowych, pod kątem adekwatności danych, do celów oraz ograniczenie dostępu do danych i ograniczenie czasu przechowywania danych.

Koordynator Ochrony Danych Osobowych – w celu efektywnego nadzoru nad przetwarzaniem Danych Osobowych Knowit PL ustanowił funkcję niezależnego eksperta z zakresu ochrony Danych Osobowych.

Inwentaryzacja danych – Knowit PL dokonuje identyfikacji zasobów Danych Osobowych w Knowit PL, kategorii i rodzajów danych, przepływów danych w organizacji i na zewnątrz oraz identyfikacji sposobów wykorzystania danych.

Rejestry Przetwarzania Danych – Knowit PL opracowuje, prowadzi i utrzymuje Rejestr Czynności Przetwarzania Danych Osobowych w Knowit PL oraz Rejestr Kategorii Czynności Przetwarzania Danych Osobowych w Knowit PL. Rejestry służą do rozliczania zgodności działania Knowit PL z przepisami o ochronie Danych Osobowych.

Podstawy przetwarzania – Knowit PL zapewnia, identyfikuje oraz weryfikuje podstawy prawne przetwarzania Danych Osobowych i dokonuje ich rejestracji je w Rejestrach, w tym:

a) zarządza zgodami na przetwarzanie Danych Osobowych;
b) uzasadnia przypadki, gdy Knowit PL przetwarza Dane Osobowe na podstawie prawnie uzasadnionego interesu Spółki.

Realizacja praw jednostki – Knowit PL spełnia obowiązki informacyjne względem osób, których dane przetwarza oraz zapewnia realizację ich praw wynikających z RODO.

Bezpieczeństwo – Knowit PL zapewnia odpowiedni poziom bezpieczeństwa Danych Osobowych, 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 Osobowych do ustalonego ryzyka;
d) zarządza bezpieczeństwem informacji;
e) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego Naruszenia Prezesowi Urzędu Ochrony Danych Osobowych oraz osobom, których dane dotyczą (Procedura Obsługi Naruszeń).

Powierzenie przetwarzania – Knowit PL posiada zasady doboru podmiotów przetwarzających dane na rzecz Knowit PL, określa wymogi co do warunków przetwarzania (umowa powierzenia przetwarzania danych) oraz zasady weryfikacji wykonywania umów powierzenia.

Przekazywanie danych do państw trzecich – Knowit PL dokonuje weryfikacji tego, czy odbiorcy Danych Osobowych nie planują transferu Danych Osobowych do państw trzecich (poza EOG, tj. UE, Norwegię, Lichtenstein, Islandię) lub do organizacji międzynarodowych. W przypadku pozytywnej weryfikacji, Knowit PL zapewnia przestrzeganie warunków przekazywania Danych Osobowych do państw trzecich zgodnie z RODO

4. PROJEKTOWANIE PRYWATNOŚCI (*PRIVACY BY DESIGN*)

1. Knowit PL zapewnia, aby w każdym obszarze prowadzonej działalności uwzględniane były zasady dotyczące ochrony prywatności i przetwarzania Danych Osobowych. W tym celu Knowit PL stale kontroluje oraz, w miarę zidentyfikowanych potrzeb, modyfikuje istniejące procesy.
2. W przypadku uruchamiania nowych projektów i inwestycji w Knowit PL, dokonywana jest oceny wpływu zmiany na ochronę Danych Osobowych, analizę ryzyka, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji lub na początku nowego projektu.
3. Zasada *privacy by design* realizowana jest przez zapewnienie audytów istniejących procesów pod kątem ochrony Danych Osobowych oraz zapewnienie udziału eksperta z zakresu ochrony Danych Osobowych w pracach dotyczących nowego projektu lub planowanej inwestycji.

5. MINIMALIZACJA (*PRIVACY BY DEFAULT*)

Knowit PL dba o minimalizację przetwarzania Danych Osobowych pod kątem adekwatności Danych Osobowych do celów przetwarzania, dostępu do Danych Osobowych oraz czasu przechowywania Danych Osobowych.

1. **Minimalizacja zakresu**

   Knowit PL zweryfikowała zakres pozyskiwanych Danych Osobowych oraz zakres ich przetwarzania pod względem adekwatności do celów przetwarzania w ramach wdrożenia RODO.

   Knowit PL dokonuje okresowych przeglądów wewnętrznych procesów obejmujących przetwarzanie Danych Osobowych nie rzadziej niż raz w roku.

2. **Minimalizacja dostępu**

Knowit PL stosuje ograniczenia dostępu do Danych Osobowych: prawne (zobowiązania do poufności, zakresy upoważnień), fizyczne (strefy dostępu, zamykanie pomieszczeń) i logiczne (ograniczenia uprawnień do systemów i zasobów, w których przetwarzane są Dane Osobowe).

Knowit PL stosuje kontrolę dostępu fizycznego. Knowit PL dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie Personelu i zmianach ról osób oraz zmianach Podmiotów Przetwarzających.

Knowit PL dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz w roku.

Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w procedurach bezpieczeństwa fizycznego i bezpieczeństwa informatycznego (IS/IT) Knowit PL.

3. **Minimalizacja czasu**

Knowit PL wdraża mechanizmy kontroli cyklu życia Danych Osobowych w Knowit PL, w tym weryfikacji dalszej przydatności danych względem terminów wskazanych w polityce retencji Danych Osobowych.

Dane, których przydatności wygasa wraz z upływem czasu, są usuwane z nośników tradycyjnych (dokumentacja papierowa) oraz cyfrowych (urządzenia i systemy IT).

6. KOORDYNATOR OCHRONY DANYCH OSOBOWYCH (*DATA PROTECTION COORDINATOR*)

1. W celu efektywnego nadzoru nad przetwarzaniem Danych Osobowych w Knowit PL utworzono niezależną funkcję Koordynatora Ochrony Danych Osobowych (KODO), który jest niezwłocznie włączany we wszystkie sprawy dotyczące ochrony Danych Osobowych.
2. Do zadań KODO należą:
   a) informowanie Knowit PL oraz Pracowników i Współpracowników, którzy przetwarzają Dane Osobowe, o obowiązkach spoczywających na nich zgodnie z RODO i dalszymi przepisami o ochronie Danych Osobowych i doradzanie im w tej sprawie;
   b) monitorowanie przestrzegania RODO, innych przepisów o ochronie Danych Osobowych oraz polityk, procedur i regulaminów Knowit PL z zakresu ochrony Danych Osobowych, w tym dotyczących obowiązków spoczywających na Personelu i właścicielach procesów biznesowych obejmujących przetwarzanie Danych Osobowych;
   c) podejmowanie działań zwiększających świadomość z zakresu ochrony Danych Osobowych, organizacja szkoleń Personelu uczestniczącego w operacjach przetwarzania oraz przeprowadzanie audytów ochrony Danych Osobowych;
   d) udzielanie, na wniosek właścicieli procesów biznesowych obejmujących przetwarzanie Danych Osobowych, zaleceń co do oceny skutków danego przedsięwzięcia dla ochrony Danych Osobowych oraz monitorowanie jej wykonania;
   e) współpraca z Organami Nadzorczymi, w tym PUODO;
   f) pełnienie funkcji osoby kontaktowej dla Organu Nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, a także, w stosownych przypadkach, prowadzenie konsultacji we wszelkich innych sprawach.
3. KODO wypełnia swoje zadania z uwzględnieniem ryzyka związanego z operacjami przetwarzania Danych Osobowych, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

4. Knowit PL wspiera KODO w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do Danych Osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.
5. Działania KODO mogą być wspierane przez podległy KODO Zespół Ochrony Danych Osobowych.
6. Knowit PL zapewnia, by KODO nie otrzymywał instrukcji dotyczących wykonywania jego zadań. Nie jest on odwoływany ani karany za wypełnianie swoich zadań. KODO bezpośrednio podlega zarządowi Knowit PL.
7. Osoby, których dane dotyczą, mogą kontaktować się z KODO we wszystkich sprawach związanych z przetwarzaniem ich Danych Osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.
8. KODO jest zobowiązany do zachowania tajemnicy i poufności co do wykonywania swoich zadań.
9. KODO nadzoruje prowadzenie następujących rejestrów:
   a) Rejestr Czynności Przetwarzania Danych (RCPD);
   b) Rejestr Kategorii Czynności Przetwarzania (RKCP);
   c) Rejestr Naruszeń;
   d) Rejestr Żądań osób, których dane dotyczą.
10. KODO może wykonywać inne zadania i obowiązki. Knowit PL zapewnia, by takie zadania i obowiązki nie powodowały konfliktu interesów oraz nie uniemożliwiały wypełniania przez KODO jego podstawowych obowiązków w zakresie nadzoru nad ochroną Danych Osobowych w Knowit PL.
11. Pracownicy oraz jednostki organizacyjne w ramach Knowit PL obowiązani są wspierać KODO w wykonywaniu zadań, a także postępować zgodnie z Polityką Ochrony Danych Osobowych oraz wskazówkami i rekomendacjami KODO w zakresie przetwarzania Danych Osobowych.

7. INWENTARYZACJA

1. Knowit PL dokonuje identyfikacji zasobów Danych Osobowych w Knowit PL, kategorii i rodzajów danych, przepływów danych w organizacji i na zewnątrz oraz identyfikacji sposobów wykorzystania danych.
2. Knowit PL identyfikuje przypadki, w których przetwarza lub może przetwarzać szczególne kategorie danych lub dane dotyczące wyroków skazujących i naruszeń prawa oraz zapewnia szczególne środki organizacyjne i bezpieczeństwa w stosunku do takich danych.
3. Knowit PL identyfikuje przypadki, w których dokonuje profilowania przetwarzanych Danych Osobowych i utrzymuje mechanizmy zapewniające zgodność tego procesu z prawem.
4. Knowit PL identyfikuje przypadki współadministrowania danymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami. W szczególności dotyczy to sytuacji współadministrowania danych w ramach grupy spółek Knowit.

8. REJESTRY PRZETWARZANIA DANYCH

1. Knowit PL prowadzi Rejestr Czynności Przetwarzania Danych („**RCPD**") oraz Rejestr Kategorii Czynności Przetwarzania Danych („**RKCP**") (łącznie zwane dalej „**Rejestrami**"). Rejestry służą do rozliczania zgodności działania Knowit PL z przepisami o ochronie Danych Osobowych. Stanowią formę dokumentowania czynności przetwarzania danych, pełnią rolę mapy przetwarzania danych i są jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.
2. Rejestry prowadzone są w formie elektronicznej.
3. W RCPD Knowit PL inwentaryzuje i monitoruje sposób, w jaki wykorzystuje Dane Osobowe jako Administrator.
4. W RCPD dla każdej czynności przetwarzania danych, którą Knowit PL uznała za odrębny proces w ramach swojej organizacji, Knowit PL odnotowuje co najmniej:
   a) nazwę czynności/procesu,
   b) cel przetwarzania,
   c) opis kategorii osób, których dane są przetwarzane w procesie,
   d) opis kategorii danych,
   e) podstawę prawną przetwarzania wraz z wyszczególnieniem uzasadnionego interesu Knowit PL, jeżeli podstawą jest uzasadniony interes,
   f) sposób zbierania danych,
   g) opis kategorii odbiorców danych (w tym Podmiotów Przetwarzających),
   h) informację o przekazaniu danych poza EU / EOG,
   i) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków ochrony danych.
5. W RKCP Knowit PL inwentaryzuje i monitoruje sposób, w jaki wykorzystuje Dane Osobowe jako Podmiot Przetwarzający.
6. W RKCP Knowit PL wyodrębnia poszczególne kategorie czynności przetwarzania, które wykonuje w imieniu innego Administratora jako Podmiot Przetwarzający lub w imieniu innego Podmiotu Przetwarzającego jako dalszy Podmiot Przetwarzający. W RKCP, Knowit PL odnotowuje co najmniej:
   a) nazwę kategorii przetwarzań dokonywanych w imieniu innego Administratora lub Podmiotu Przetwarzającego,
   b) nazwę każdego Administratora oraz Podmiotu Przetwarzającego, w imieniu którego działa Knowit PL;
   c) cel przetwarzania,
   d) opis kategorii osób, których dotyczy przetwarzanie,
   e) opis kategorii danych,
   f) podstawę przetwarzania (informację o zawarciu umowy powierzenia przetwarzania),
   g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków ochrony danych.

9. PODSTAWY PRZETWARZANIA

1. Knowit PL opisuje w Rejestrze Czynności Przetwarzania Danych (RCPD) podstawy prawne przetwarzania Danych Osobowych dla poszczególnych czynności (procesów) przetwarzania.
2. Wskazując podstawę prawną (Zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne / władza publiczna, prawnie uzasadniony cel Knowit PL), Knowit PL dookreśla podstawę w precyzyjny i czytelny sposób.
3. Knowit PL wdraża metody zarządzania Zgodami umożliwiające rejestrację i weryfikację posiadania Zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na kierowanie marketingu bezpośredniego z wykorzystaniem telekomunikacyjnych urządzeń końcowych (telefon, tablet, komputer), zgody na przesyłanie informacji handlowych z wykorzystaniem środków komunikacji elektronicznej (e-mail, SMS) oraz rejestrację cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie przetwarzania).
4. Kierownik każdej jednostki organizacyjnej i właściciel każdego procesu biznesowego w Knowit PL ma obowiązek znać podstawy prawne, na jakich kierowana przez niego jednostka lub prowadzony proces dokonuje konkretnych czynności przetwarzania Danych Osobowych. Jeżeli podstawą jest uzasadniony interes Knowit PL, kierownik jednostki ma obowiązek znać konkretny interes Knowit PL, któremu służyć ma przetwarzanie danych.

10. SPOSÓB REALIZACJI PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ, W TYM OBOWIĄZKÓW INFORMACYJNYCH

1. Knowit PL dba o przejrzystość, czytelność i dostępność przekazywanych informacji oraz komunikacji z osobami, których Dane Osobowe przetwarza.
2. Knowit PL ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym zamieszczenie na stronie internetowej Knowit PL informacji lub linków do informacji o przetwarzaniu Danych Osobowych, prawach osób, sposobie skorzystania z przysługujących praw w Knowit PL, w tym wymaganiach dotyczących weryfikacji tożsamości oraz metodach kontaktu z Knowit PL w tym celu.
3. Knowit PL dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób, których dane dotyczą.
4. W celu realizacji praw jednostki Knowit PL zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Knowit PL, zintegrować te dane, wprowadzać do nich zmiany i usuwać.

11. OBOWIĄZKI INFORMACYJNE

1. Knowit PL informuje osoby, których dane dotyczą o przetwarzaniu ich Danych Osobowych oraz przysługujących takim osobom prawach związanych z ochroną danych, przy pozyskiwaniu danych od tych osób.
2. Knowit PL informuje osoby, których dane pozyskała w sposób inny niż od osoby, której dotyczą, niezwłocznie – nie później niż w ciągu miesiąca od pozyskania danych, a w przypadku, gdy Dane Osobowe mają być wykorzystywane do komunikacji z takimi osobą – przy pierwszej komunikacji

z tymi osobą. W przypadku, gdy dane mają zostać ujawnione innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.

3. Tam, gdzie jest to możliwe, Knowit PL określa sposób informowania osób o przetwarzaniu danych nieidentyfikujących konkretnej osoby (np. tabliczka o objęciu obszaru monitoringiem wizyjnym).
4. Knowit PL informuje osoby, których dane dotyczą o planowanej zmianie celu przetwarzania Danych Osobowych.
5. Knowit PL informuje osoby, których dane dotyczą przed uchyleniem ograniczenia przetwarzania.
6. Knowit PL informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to niemożliwe lub będzie wymagało niewspółmiernie dużego wysiłku).
7. Knowit PL informuje osoby, których dane dotyczą o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tymi osobami.
8. Knowit PL informuje osoby, których dane dotyczą o prawie do wycofania w dowolnym momencie Zgody na przetwarzanie danych w określonym celu najpóźniej podczas pozyskiwania Zgody
9. Knowit PL bez zbędnej zwłoki zawiadamia osoby, których dane dotyczą o naruszeniu ochrony danych osobowych, jeżeli może ono spowodować wysokie ryzyko naruszenia praw lub wolności tych osób, zgodnie z Procedurą Obsługi Naruszeń stanowiącą Załącznik nr 2 do Polityki.

12. ŻĄDANIA OSÓB, KTÓRYCH DANE DOTYCZĄ

1. Knowit PL realizuje prawa osób, których dane dotyczą, określone w art. 15-22 RODO, zgodnie z Procedurą Obsługi Żądań stanowiącą Załącznik nr 1 do POD.
2. Realizując prawa osób, których dane dotyczą, Knowit PL wprowadza 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), Knowit PL może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia Żądaniu.

13. BEZPIECZEŃSTWO

Knowit PL zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania Danych Osobowych przez Knowit PL.

1. **Analiza ryzyka i adekwatności środków bezpieczeństwa**
   Knowit PL przeprowadza analizy adekwatności środków bezpieczeństwa Danych Osobowych. W tym celu:
   a) Knowit PL zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania – wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych;

b) Knowit PL kategoryzuje Dane Osobowe oraz czynności przetwarzania pod względem ryzyka, które przedstawiają;

c) Knowit PL przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania Danych Osobowych lub ich kategorii; Knowit PL 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;

d) Knowit PL ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa Danych Osobowych przy uwzględnieniu racjonalnego kosztu ich wdrażania. Knowit PL ustala przydatność i w uzasadnionych przypadkach stosuje takie środki i podejście jak:
   - pseudonimizacja;
   - szyfrowanie;
   - inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
   - 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.

2. **Ocena skutków dla ochrony Danych Osobowych (DPIA)**
   Knowit PL dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony Danych Osobowych tam, gdzie zgodnie z analizą ryzyka, ryzyko naruszenia praw i wolności osób jest wysokie.

3. **Środki bezpieczeństwa**
   Knowit PL stosuje środki bezpieczeństwa ustalone w ramach analizy ryzyka i adekwatności środków bezpieczeństwa oraz oceny skutków dla ochrony Danych Osobowych.
   Środki bezpieczeństwa Danych Osobowych przetwarzanych w środowisku IT stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa w Knowit PL i są opisane w procedurze bezpieczeństwa informatycznego (IS/IT) w Knowit PL.

4. **Obsługa naruszeń**
   Knowit PL stosuje procedurę pozwalającą na identyfikację, ocenę i – tam, gdzie okaże się to niezbędne – zgłoszenie zidentyfikowanego Naruszenia ochrony danych Prezesowi Urzędu Ochrony Danych (Zawiadomienie PUODO) lub osobie, której dane dotyczą (Zawiadomienie PD), a także minimalizację negatywnych skutków naruszenia i ustalenie na przyszłość działań w celu uniknięcia ponownego wystąpienia tego rodzaju zdarzenia.

14. PODMIOT PRZETWARZAJĄCY

1. Knowit PL dokonuje weryfikacji Podmiotów Przetwarzających Dane Osobowe w imieniu Knowit PL 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 Osobowych spoczywających na Knowit PL.

2. Knowit PL zawiera z Podmiotami Przetwarzającymi umowy zgodnie z wymogami określonymi w art. 28 RODO.
3. Knowit PL rozlicza Podmioty Przetwarzające z wykorzystania dalszych podmiotów przetwarzających przez zapewnienie uprawnień kontrolnych (bezpośrednio lub za pośrednictwem Podmiotu Przetwarzającego).

15. PRZEKAZYWANIE DANYCH DO PAŃSTW TRZECICH I ORGANIZACJI MIĘDZYNARODOWYCH

1. Knowit PL rejestruje w RCPD przypadki przekazywania Danych Osobowych do państw trzecich, to jest poza Europejski Obszar Gospodarczy (kraje Unii Europejskie, Islandia, Liechtenstein i Norwegia).
2. W przypadku planowanego przetwarzania Danych Osobowych w państwach trzecich, Knowit zapewnia przestrzeganie warunków przekazywania Danych Osobowych do państw trzecich zgodnie z RODO, w szczególności na podstawie umowy uwzględniającej wymogi UE w zakresie przekazywania Danych Osobowych poza teren EOG, takie jak standardowe klauzule umowne zatwierdzone przez Komisję Europejską.

16. POSTANOWIENIA KOŃCOWE

1. Polityka Ochrony Danych Osobowych w aktualnym brzmieniu obowiązuje od dnia 10 lutego 2022 roku.

Załącznik nr 1
do Polityki Ochrony Danych Osobowych z dnia 10 lutego 2022 r.

PROCEDURA OBSŁUGI ŻĄDAŃ OSÓB, KTÓRYCH DANE DOTYCZĄ W KNOWIT POLAND SP. Z O.O.

1 stycznia 2022 r.

Knowit Poland sp. z o.o.
ul. Hrubieszowska 2
01-209 Warszawa
NIP: 951 178 99 96

Ph +48 22 355 21 70
Fax +48 22 355 21 71
www.knowit.eu

KRS 0000036076
Sąd Rejonowy dla m.st. Warszawy
XII Wydział Gospodarczy KRS
Kapitał zakładowy: 1 251 200 PLN

knowit

PROCEDURA OBSŁUGI ŻĄDAŃ OSÓB, KTÓRYCH DANE DOTYCZĄ W KNOWIT POLAND SP. Z O.O.

1. DEFINICJE

Na potrzeby Procedury obsługi żądań osób, których dane dotyczą przyjmuje się następujące definicje:

(1) „**Administrator**" – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Administratorem jest Knowit PL. W przypadku, gdy Knowit działa na zlecenie klienta, Administratorem jest klient, a Knowit występuje w roli podmiotu przetwarzającego. W określonych przypadkach Knowit PL działa jako dalszy podmiot przetwarzający dane;

(2) „**Knowit PL**" – Knowit Poland sp. z o.o. z siedzibą w Warszawie, ul. Hrubieszowska 2, 01-209 Warszawa, wpisana do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie XII Wydział Gospodarczy pod numerem KRS: 0000036076, NIP: 951-17-89-996; REGON: 01284093700000, kapitał zakładowy: 1.251.200,00 zł;

(3) „**Dane Osobowe**" lub „**dane**" – oznaczają 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, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

(4) „**Koordynator Ochrony Danych Osobowych**", „**KODO**" lub „**Data Protection Coordinator**" – ustanowiona w Knowit PL funkcja niezależnego eksperta z zakresu ochrony Danych Osobowych nadzorującego przetwarzanie Danych Osobowych w Knowit PL;

(5) „**Naruszenie**" – 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;

(6) „**Personel**" – oznacza Pracowników i Współpracowników Knowit PL;

(7) „**Prezes Urzędu Ochrony Danych Osobowych**" lub „**PUODO**" – oznacza właściwy organ administracji publicznej odpowiedzialny za realizację zadań w zakresie ochrony Danych Osobowych;

(8) „**Pracownik**" – oznacza osobę związaną stosunkiem pracy z Knowit PL;

(9) „**Procedura Obsługi Żądań**", „**Procedura**" lub „**POŻ**" – oznacza niniejszą procedurę postępowania w przypadku zgłoszenia żądania przez osobę, której dane dotyczą obowiązującą w Knowit PL;

(10) „**Rejestr Żądań**" – oznacza rejestr żądań zgłoszonych do Knowit PL przez osoby, których dane dotyczą związanych z realizacją ich uprawnień wynikających z art 15-22 RODO, o którym mowa w Punkcie 5 poniżej;

(11) „**RODO**" – oznacza 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 (ogólne rozporządzenie o ochronie danych) (Dz.U. UE. L. z 2016 r. Nr 119, str. 1);

(12) „**Współpracownik**" – oznacza osobę związaną z Knowit PL stosunkiem zlecenia lub innej umowy cywilnoprawnej, a także praktykanta i stażystę;

(13) „**Żądanie**" – skierowane do Knowit PL przez osobę, której dane dotyczą, żądanie związane z realizacją uprawnień wynikających z art 15-22 RODO.

2. CEL I ZAKRES PROCEDURY

1. W celu zapewnienia efektywnego działania w zakresie obsługi Żądań osób, których dane dotyczą zgodnie z wymogami RODO, przyjmuje się niniejszą Procedurę Obsługi Żądań.
2. Procedura Obsługi Żądań reguluje:
   (1) zasady postępowania w przypadku zgłoszenia Żądania,
   (2) zasady prowadzenia Rejestru i dokumentacji związanej z obsługą Żądań.

3. OBOWIĄZKI PERSONELU ZWIĄZANE Z OBSŁUGĄ ŻĄDAŃ

1. Każdy Pracownik i Współpracownik obowiązany jest do zapoznania się i stosowania Procedury Obsługi Żądań.
2. Każdy Pracownik i Współpracownik, pozyskawszy wiadomość o Żądaniu, ma obowiązek natychmiast zawiadomić o tym fakcie ustnie lub w formie wiadomości e-mail swojego bezpośredniego przełożonego oraz KODO. Zawiadomienie KODO należy przesłać na adres e-mail: dataprotection@knowitgroup.com.
3. Żądania, które należy zgłosić bezpośredniemu przełożonemu oraz KODO obejmują w szczególności następujące przypadki:
   (1) żądanie udostępnienia danych (uzyskania informacji o przetwarzaniu Danych Osobowych dotyczących danej osoby);
   (2) żądanie uzyskania kopii danych;
   (3) żądanie sprostowania lub uzupełnienia danych;
   (4) żądanie usunięcia danych („prawo do bycia zapomnianym");
   (5) żądanie ograniczenia przetwarzania;
   (6) żądanie przeniesienia danych do innego Administratora;
   (7) żądanie zaprzestania przetwarzania Danych Osobowych w celach marketingowych lub w innym prawnie uzasadnionym interesie Administratora (sprzeciw);
   (8) żądanie związane z zaprzestaniem podejmowania decyzji w sposób zautomatyzowany oraz profilowania.
4. Zawiadomienie, o którym mowa w Punkcie 3.2 powyżej, powinno opisywać rodzaj Żądania, datę zgłoszenia Żądania i zawierać treść Żądania, co dotyczy w szczególności Żądania złożonego ustnie przez osobę, której dane dotyczą. Żądanie w postaci utrwalonej (dokument, e-mail), należy

przesłać w wiadomości e-mail pod adres dataprotection@knowitgroup.com oraz przekazać niezwłocznie oryginał pisma KODO.

5. Zawiadomienia, o którym mowa w Punkcie 3.2 powyżej, należy dokonać najpóźniej w ciągu 24 (dwudziestu czterech) godzin od chwili pozyskania wiadomości o Żądaniu.
6. Każdy Pracownik i Współpracownik obowiązany jest do udzielania przełożonemu i KODO wszelkich wyjaśnień związanych ze złożonym Żądaniem, w szczególności poprzez zapewnienie dostępu do informacji, materiałów, dokumentów lub narzędzi informatycznych. Pracownik i Współpracownik obowiązany jest udzielić wyjaśnień niezwłocznie, nie później jednak niż w terminie 2 dni roboczych od przesłania zapytania.

4. OBOWIĄZKI KODO ZWIĄZANE Z OBSŁUGĄ NARUSZEŃ

1. KODO:
   (1) nadzoruje przestrzeganie w Knowit PL przepisów o ochronie danych osobowych, w tym związanych z obsługą Żądań osób, których dane dotyczą;
   (2) obsługuje skrzynkę kontaktową utworzoną m.in. do kierowania Żądań: dataprotection@knowitgroup.com ;
   (3) koordynuje działania w celu udzielenia odpowiedzi osobie, której dane dotyczą, a w uzasadnionych przypadkach, zrealizowania Żądania;
   (4) prowadzi Rejestr Żądań;
   (5) koordynuje prace związane z wprowadzeniem środków organizacyjnych i technicznych ułatwiających realizację Żądań osób, których dane dotyczą.

5. REJESTR

1. KODO prowadzi Rejestr Żądań w formie elektronicznej.
2. KODO decyduje o umieszczeniu zawiadomienia, o którym mowa w Punkcie 3.2 powyżej, w Rejestrze. Wpisowi podlegają jedynie Żądania wynikające z uprawnień przewidzianych w art. 15-22 RODO.
3. Wpis do Rejestru powinien zawierać:
   (1) opis Żądania;
   (2) datę zgłoszenia Żądania;
   (3) informacja o weryfikacji osoby składającej Żądanie;
   (4) informację dotyczącą realizacji Żądania lub powodów, dla których Żądanie nie mogło zostać zrealizowane;
   (5) datę udzielenia odpowiedzi osobie, której dane dotyczą.

6. WERYFIKACJA TOŻSAMOŚCI

1. W przypadku zgłoszenia Żądania, przez osobę, której dane dotyczą, należy dokonać weryfikacji składającego Żądanie. Weryfikacja tożsamości jest konieczna w celu uniknięcia udzielenia odpowiedzi osobie nieuprawnionej lub realizacji Żądania pochodzącego od osoby nieuprawnionej, co stanowi Naruszenie ochrony Danych Osobowych.

2. Weryfikacja osoby składającej Żądanie należy do KODO lub innej osoby wyznaczonej do realizacji Żądania. W przypadku braku danych umożliwiających weryfikację tożsamości lub realizację Żądania, konieczny jest dalszy kontakt z osobą składającą Żądanie w celu wyjaśnienia wątpliwości. Preferowaną formą kontaktu jest kontakt za pośrednictwem poczty e-mail. W przypadku kontaktu telefonicznego, konieczne jest sporządzenie notatki służbowej z rozmowy, opisującej jej przebieg.
3. Po dokonaniu pozytywnej weryfikacji, możliwe jest przystąpienie do dalszego etapu obsługi Żądania, opisanego w punkcie 7 Procedury.
4. W przypadku negatywnej weryfikacji, KODO lub osoba wyznaczona do obsługi Żądania wysyła do osoby składającej Żądanie informację o braku możliwości rozpatrzenia Żądania.
5. Informacja o wyniku weryfikacji zostaje umieszczona w Rejestrze Żądań.
6. Jeżeli na podstawie weryfikacji ustalono, że Żądanie zostało złożone przez osobę, której dane osobowe są przetwarzane przez Knowit PL w imieniu innego Administratora lub Podmiotu Przetwarzającego, informacja o Żądaniu zostaje niezwłocznie przekazana przez KODO lub osobę wyznaczoną do obsługi Żądania do właściwego Administratora lub Podmiotu Przetwarzającego, na zlecenie którego działa Knowit PL zgodnie z Punktem 8 Procedury.

7. OBSŁUGA ŻĄDANIA

1. Po dokonaniu pozytywnej weryfikacji osoby składającej Żądanie oraz ustaleniu zakresu Żądania, KODO lub osoba wyznaczona do obsługi Żądania, informuje osobę, która złożyła Żądanie o przystąpieniu do analizy zasadności Żądania i jego realizacji w formie wiadomości e-mail lub pisemnie, w zależności od ustalonego sposobu komunikacji.
2. KODO lub osoba wyznaczona do obsługi Żądania przeprowadza analizę treści Żądania i dokonuje analizy zasadności Żądania zgodnie z art. 15-22 RODO. Ocena zasadności Żądania powinna zostać dokonana indywidualnie w każdym przypadku z uwzględnieniem wskazówek zawartych w załączniku do Procedury: „Uprawnienia osób, których dane dotyczą – *Poradnik reagowania na żądania*."
3. W przypadku gdy Żądanie nie znajduje podstaw w przepisach prawa, KODO lub osoba wyznaczona do obsługi Żądania informuje osobę, która złożyła Żądanie o przyczynach, dla których Żądanie nie może zostać zrealizowane.
4. Jeżeli ustalono, iż istnieją podstawy do zrealizowania Żądania, KODO lub osoba wyznaczona do obsługi Żądania, koordynuje prace w Knowit PL w celu niezwłocznej realizacji Żądania z uwzględnieniem wskazówek zawartych w załączniku do Procedury: „Uprawnienia osób, których dane dotyczą – *Poradnik reagowania na żądania*."
5. Knowit PL bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania Żądania – udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z Żądaniem. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter Żądania lub liczbę Żądań. W terminie miesiąca od otrzymania żądania Knowit PL informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie

elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.

6. Jeżeli Knowit PL nie podejmuje działań w związku z Żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania Żądania – informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych oraz skorzystania ze środków ochrony prawnej przed sądem.
7. Komunikacja i działania podejmowane w związku z wniesionym Żądaniem są wolne od opłat. Jeżeli Żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, Knowit PL może:
   (1) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo
   (2) odmówić podjęcia działań w związku z Żądaniem.

   Obowiązek wykazania, że Żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na Knowit PL.

8. ŻĄDANIA DOTYCZĄCE DANYCH PRZETWARZANYCH W IMIENIU INNYCH ADMINISTRATORÓW LUB PODMIOTÓW PRZETWARZAJĄCYCH

1. W przypadku gdy na podstawie analizy Żądania zostanie ustalone, iż Żądanie dotyczy Danych Osobowych przetwarzanych przez Knowit PL w imieniu innego Administratora lub gdy Knowit PL będzie działał jako dalszy Podmiot Przetwarzający, Knowit PL niezwłocznie zawiadomi o Żądaniu właściwego Administratora lub Podmiot Przetwarzający, a także poinformuje osobę, która złożyła Żądanie o przekazaniu Żądania innemu podmiotowi i przyczynach takiego postępowania.
2. W opisanym procesie zastosowanie mają tryb i terminy zawiadomień przewidziane w umowach powierzenia przetwarzania Danych Osobowych zawartych przez Knowit PL z kontrahentami będącymi Administratorami lub Podmiotami Przetwarzającymi.
3. Uwzględniając charakter przetwarzania oraz dostępne Knowit PL informacje, Knowit PL będzie wspierał właściwego Administratora lub Podmiot Przetwarzający w zakresie obowiązków, które podmioty te posiadają dotyczących realizacji Żądań.

9. POSTANOWIENIA KOŃCOWE

1. Integralną część niniejszej Procedury stanowi załącznik: „*Uprawnienia osób, których dane dotyczą – Poradnik reagowania na żądania*."
2. Procedura wchodzi w życie z dniem 1 stycznia 2022 r.

knowit

Załącznik nr 1

UPRAWNIENIA OSÓB, KTÓRYCH DANE DOTYCZĄ
PORADNIK REAGOWANIA NA ŻĄDANIA W KNOWIT POLAND SP. Z O.O.

LISTA UPRAWNIEŃ

Niniejsza broszura zawiera syntetyczne zestawienie uprawnień osób, których dane dotyczą, oraz związanych z nimi obowiązków administratorów danych na gruncie 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 (ogólne rozporządzenie o ochronie danych) („**RODO**").

RODO przewiduje następujące uprawnienia osób, których dane dotyczą:

1) **prawo dostępu do danych** (w tym prawo do uzyskania informacji o przetwarzaniu oraz prawo do uzyskania kopii danych);
2) **prawo do sprostowania lub uzupełnienia danych**;
3) **prawo do usunięcia danych** („prawo do bycia zapomnianym");
4) **prawo do ograniczenia przetwarzania**;
5) **prawo do przeniesienia danych**;
6) **prawo do sprzeciwu**;
7) **prawa związane ze zautomatyzowanym podejmowaniem decyzji, w tym profilowaniem**.

OGÓLNE ZASADY DOTYCZĄCE REALIZOWANIA ŻĄDAŃ PODMIOTÓW DANYCH

RODO przewiduje, że realizacja Żądań osób, których dane dotyczą (realizujących swoje uprawnienia) powinna następować zgodnie z wymienionymi niżej zasadami. Zasady te mają zastosowanie do wszystkich omówionych w niniejszej broszurze praw osób, których dane dotyczą.

Przejrzysta komunikacja

Administrator powinien podejmować odpowiednie środki, aby wszelka komunikacja prowadzona z podmiotem danych w związku ze zgłoszonym przez niego Żądaniem (oraz realizacja tego Żądania) była prowadzona w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem (w szczególności, gdy komunikacja prowadzona jest z dzieckiem).

W przypadku uprawnień polegających na udzieleniu informacji, informacji udziela się na piśmie lub w inny sposób, w tym elektronicznie. Jednakże ustne udzielenie informacji może nastąpić tylko wtedy, gdy zażąda tego osoba, której dane dotyczą i tylko wtedy gdy innymi sposobami potwierdzi się tożsamość tej osoby.

Termin na realizację Żądań

Realizacja Żądania (a przynajmniej poinformowanie o działaniach podjętych w związku z Żądaniem) musi nastąpić **bez zbędnej zwłoki**, nie później jednak niż w terminie **miesiąca** od otrzymania Żądania.

Ze względu na skomplikowany charakter Żądania lub liczbę żądań, w razie potrzeby, Administrator danych może **przedłużyć** ten termin do maksymalnie **trzech miesięcy** od otrzymania Żądania – nawet

wtedy jest jednak zobowiązany w terminie **miesiąca** od jego otrzymania poinformować osobę, która wystąpiła z Żądaniem, o przedłużeniu oraz podać przyczyny opóźnienia.
Jeżeli Administrator nie podejmuje działań w związku z Żądaniem, to **niezwłocznie**, najpóźniej w terminie **miesiąca** od otrzymania Żądania, informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego (Prezesa Urzędu Ochrony Danych Osobowych).
Jeżeli Żądanie zostało przekazane elektronicznie, powyższe informacje powinny – w miarę możliwości – również być przekazywane elektronicznie (chyba że osoba, której dane dotyczą, sama zażąda innej formy).

Zakaz pobierania opłat

Wszelkie informacje, komunikacja i działania podejmowane w wykonaniu Żądań uprawnionych osób są **wolne od opłat**.
Na zasadzie **wyjątku** Administrator może pobrać **rozsądną opłatę**, uwzględniającą administracyjne koszty komunikacji lub podjęcia żądanych działań, tylko wtedy, gdy wykaże, że żądania danej osoby są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój nadmierny charakter (np. cykliczne występowanie z tym samym Żądaniem w krótkich odstępach czasu). W takim wypadku Administrator może też odmówić realizacji Żądania (o czym niżej). Aby nie narazić się na odpowiedzialność Administrator musi jednak później umieć wykazać, że Żądanie istotnie było nieuzasadnione lub nadmierne.

Brak możliwości odmowy

Administrator zobowiązany jest ułatwiać osobie, której dane dotyczą, wykonanie przysługujących jej uprawnień. Administrator nie odmawia podjęcia działań na Żądanie osoby pragnącej wykonać przysługujące jej prawa nawet wtedy, gdy chodzi o przetwarzanie niewymagające identyfikacji danej osoby (ze względu na cele przetwarzania), chyba że wykaże, że nie jest w stanie zidentyfikować osoby, której dane dotyczą.
Na zasadzie **wyjątku** Administrator może odmówić podjęcia działań w związku z Żądaniem, tylko wtedy, gdy wykaże, że Żądania danej osoby są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter (np. cykliczne występowanie z tym samym żądaniem w krótkich odstępach czasu). Aby nie narazić się na odpowiedzialność administrator musi jednak później umieć wykazać, że Żądanie istotnie było nieuzasadnione lub nadmierne.

Możliwość weryfikacji tożsamości

W przypadkach gdy Administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej Żądanie (związane z realizacją któregokolwiek z praw), może **zażądać dodatkowych informacji niezbędnych** do potwierdzenia tożsamości osoby, której dane dotyczą.

knowit

1. PRAWO DOSTĘPU DO DANYCH

Podstawa prawna: art. 15 RODO

Treść Żądania:

- żądanie **potwierdzenia**, czy Administrator przetwarza dane tej osoby;
- żądanie uzyskania **dostępu** do danych;
- żądanie uzyskania następujących **informacji**:
  - cele przetwarzania;
  - kategorie odnośnych Danych Osobowych;
  - informacje o odbiorcach lub kategoriach odbiorców, którym dane zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
  - w miarę możliwości planowany okres przechowywania danych, a gdy jego podanie nie jest możliwe, kryteria ustalania tego okresu;
  - informacja o prawie do żądania od Administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych dotyczących tej osoby, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
  - informacja o prawie wniesienia skargi do Organu Nadzorczego (PUODO);
  - gdy dane nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
  - informacje o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu, oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą;
  - gdy dane są przekazywane do państwa trzeciego lub organizacji międzynarodowej – informacje o odpowiednich zabezpieczeniach związanych z takim przekazaniem, o których mowa w art. 46 RODO;
- żądanie otrzymania **kopii** wszelkich danych podlegających przetwarzaniu przez Administratora.

Zakres obowiązków Administratora:

- sprawdzenie i w razie odpowiedzi twierdzącej **potwierdzenie**, że Administrator przetwarza Dane Osobowe osoby żądającej;
- zapewnienie osobie, której dane dotyczą, **dostępu** do tych danych (np. poprzez profil użytkownika, zdalny dostęp do danych lub udostępnienie danych w inny sposób);
- podanie – na żądanie osoby – **informacji** wyżej wymienionych;
- dostarczenie osobie, której dane dotyczą, kopii Danych Osobowych podlegających przetwarzaniu przez Administratora (RODO nie określa tu formy takiej kopii, może to być np. plik PDF lub inny zawierający kopię danych)

Sposób realizacji Żądania:
Wyżej wymieniona żądania muszą być realizowane bez jakichkolwiek opłat na rzecz Administratora. Jednakże w przypadku żądania dostarczenia kopii danych, wolna od opłat jest tylko pierwsza kopia. Za wszelkie kolejne kopie, o które zwróci się podmiot danych, Administrator może pobrać opłatę w rozsądnej wysokości wynikających z kosztów administracyjnych (np. realny koszt przygotowania i wytworzenia takiej kopii).
Jeżeli osoba zwraca się o kopię danych drogą elektroniczną i nie zaznaczy inaczej, to kopia powinna być przekazana powszechnie stosowaną drogą elektroniczną (UWAGA: przekazanie informacji i danych musi nastąpić w sposób bezpieczny, wymagane jest np. zastosowanie szyfrowania).
Termin realizacja żądania: Bez zbędnej zwłoki, a w każdym razie w terminie miesiąca od otrzymania Żądania. W razie potrzeby istnieje możliwość przedłużenia tego terminu do trzech miesięcy, jednakże tylko z uwagi na skomplikowany charakter Żądania lub liczbę żądań (o czym należy poinformować osobę składająca Żądanie w terminie miesiąca od otrzymania Żądania). Gdy Administrator nie zamierza podjąć działań w związku z Żądaniem, informuje o tym osobę żądającą niezwłocznie, najpóźniej w terminie miesiąca od otrzymania Żądania.

2. PRAWO DO SPROSTOWANIA LUB UZUPEŁNIENIA DANYCH

Podstawa prawna: art. 16 RODO

Treść Żądania:
- żądanie niezwłocznego **sprostowania** Danych Osobowych, gdy są one nieprawidłowe;
- żądanie **uzupełnienia** niekompletnych Danych Osobowych (z uwzględnieniem celów przetwarzania) np. poprzez przedstawienie dodatkowego oświadczenia.

Zakres obowiązków Administratora:
- obowiązek sprostowania danych nieprawidłowych na żądanie danej osoby. Administrator nie ma obowiązku stałego badania, czy dane osobowe są prawidłowe, niemniej jednak gdy w toku przetwarzania danych uzyska informacje wskazującą na to, że dane są nieprawidłowe (np. błąd wysyłania maila na wskazany adres, zwrot przesyłki pocztowej ze względu na przeprowadzkę adresata), powinien podjąć działania mające na celu ich sprostowanie (np. zwrócić się w tym celu do podmiotu danych) – zgodnie z zasadą prawidłowości (art. 5 ust. 1 lit. d RODO);
- obowiązek uzupełnienia niekompletnych Danych Osobowych na żądanie danej osoby. Administrator nie ma obowiązku uzupełnienia danych o wszelkie brakujące dane osobowe (nawet gdy osoba zażąda uzupełnienia w tym zakresie), a jedynie o takie, które odpowiadają celom przetwarzania;
- w razie dokonanego sprostowania – obowiązek poinformowania o sprostowaniu każdego odbiorcy, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku (art. 19 RODO).

Sposób realizacji Żądania:
Wyżej wymieniona żądania muszą być realizowane bez jakichkolwiek opłat na rzecz Administratora.
Zakres obowiązku poinformowania o sprostowaniu danych każdego odbiorcy, któremu ujawniono Dane Osobowe, może zostać ograniczony, jeżeli administrator wykaże, że wymagałoby to niewspółmiernie dużego wysiłku.

Termin realizacji Żądania:
Żądanie sprostowania danych powinno nastąpić niezwłocznie, zaś żądanie uzupełnienia danych bez zbędnej zwłoki (choć wydaje się, że terminy te należy traktować identycznie). W obu przypadkach terminem jest jednak miesiąc od otrzymania Żądania. W razie potrzeby istnieje możliwość przedłużenia tego terminu do trzech miesięcy, jednakże tylko z uwagi na skomplikowany charakter Żądania lub liczbę żądań (o czym należy poinformować podmiot żądający w terminie miesiąca od otrzymania żądania). Gdy Administrator nie zamierza podjąć działań w związku z Żądaniem, informuje o tym osobę żądającą niezwłocznie, najpóźniej w terminie miesiąca od otrzymania Żądania.

3. PRAWO DO USUNIĘCIA DANYCH

Podstawa prawna: art. 17 RODO

Treść Żądania:
- żądanie niezwłocznego usunięcia danych

Zakres obowiązku Administratora:
- obowiązek usunięcia danych, jeżeli zachodzi jedna z następujących okoliczności:
  - dane nie są już niezbędne do celów, w których zostały zebrane/przetwarzane;
  - cofnięcie zgody (gdy przetwarzanie opiera się na zgodzie) i brak innej podstawy prawnej przetwarzania, np. przepisu szczególnego ustawy zobowiązującego do przechowywania danych przez określony czas);
  - wniesienie sprzeciwu wobec przetwarzania danych i brak nadrzędnych prawnie uzasadnionych podstaw przetwarzania;
  - dane były przetwarzane niezgodnie z prawem;
  - konieczność usunięcia w celu wywiązania się z obowiązku prawnego, któremu podlega administrator;
  - dane były zebrane w związku z oferowaniem usług społeczeństwa informacyjnego na podstawie zgody dziecka.
- w razie wcześniejszego upublicznienia danych przez Administratora – obowiązek podjęcia wszelkich rozsądnych działań, w tym środków technicznych – biorąc jednak pod uwagę dostępną technologię i koszt realizacji – aby poinformować administratorów przetwarzających te dane o

żądaniu podmiotu danych, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych oraz ich replikacje;

- w razie dokonanego usunięcia danych – obowiązek poinformowania o usunięciu danych każdego odbiorcy, któremu ujawniono Dane Osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku (art. 19 RODO). Jest to odrębny obowiązek od wyżej wymienionego – odnosi się do obiorców danych, a nie administratorów przetwarzających dane na skutek ich wcześniejszego upublicznienia przez „pierwotnego" administratora.

Sposób realizacji Żądania:

Wyżej wymieniona żądanie oraz podjęcie działań informacyjnych wobec innych administratorów i odbiorców danych muszą być realizowane bez jakichkolwiek opłat na rzecz Administratora.

Zakres obowiązku podjęcia rozsądnych działań w celu poinformowania administratorów przetwarzających dane osobowe, które zostały upublicznione, o żądaniu ich usunięcia zależny jest od dostępnej (dla danego administratora) technologii oraz kosztów realizacji takich działań.

Zakres obowiązku poinformowania o usunięciu danych każdego odbiorcy, któremu ujawniono Dane Osobowe, może zostać ograniczony, jeżeli Administrator wykaże, że wymagałoby to niewspółmiernie dużego wysiłku.

Administrator nie jest zobowiązany do usunięcia danych (wyłączenie prawa do usunięcia danych) w zakresie w jakim przetwarzanie jest niezbędne:

- do korzystania z prawa do wolności wypowiedzi i informacji;
- do wywiązania się z prawnego obowiązku wymagającego przetwarzania wynikającego z prawa unijnego lub krajowego, bądź do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi;
- z uwagi na interes publiczny w dziedzinie zdrowia publicznego;
- do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, o ile prawdopodobne jest, że żądanie usunięcia danych uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania;
- do ustalenia, dochodzenia lub obrony roszczeń.

Obowiązek wykazania, że zachodzi wyłączenie prawa do usunięcia danych obciąża Administratora.

Termin realizacja Żądania:

Bez zbędnej zwłoki, nie później jednak niż miesiąc od otrzymania Żądania. W razie potrzeby istnieje możliwość przedłużenia tego terminu do trzech miesięcy, jednakże tylko z uwagi na skomplikowany charakter Żądania lub liczbę żądań (o czym należy poinformować podmiot żądający w terminie miesiąca od otrzymania żądania). Gdy Administrator nie zamierza podjąć działań w związku z Żądaniem, informuje o tym osobę żądającą niezwłocznie, najpóźniej w terminie miesiąca od otrzymania Żądania.

4. PRAWO DO OGRANICZENIA PRZETWARZANIA

Podstawa prawna: art. 18 RODO

Treść Żądania:

- żądanie ograniczenia przetwarzania Danych Osobowych, tj. zaprzestanie przetwarzania danych, z wyjątkiem ich przechowywania. Administrator może dalej przechowywać dane, ale wszelkie inne operacje przetwarzania są niedopuszczalne

Zakres obowiązku Administratora:

- obowiązek ograniczenia przetwarzania Danych Osobowych, tj. zaprzestania przetwarzania danych, z wyjątkiem ich przechowywania, w następujących przypadkach:
  - gdy podmiot danych kwestionuje prawidłowość danych – ograniczenie na okres pozwalający Administratorowi sprawdzić ich prawidłowość;
  - gdy przetwarzanie jest niezgodne z prawem, ale podmiot danych sprzeciwia się ich usunięciu, a żąda jedynie ich ograniczenia;
  - gdy dane nie są już potrzebne do celów przetwarzania, ale są potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
  - gdy podmiot danych wniósł sprzeciw wobec przetwarzania (por. prawo do sprzeciwu) – ograniczenie do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie Administratora są nadrzędne wobec podstaw sprzeciwu tej osoby.
- w razie dokonania ograniczenia przetwarzania – Administrator może dalej przechowywać dane, ale wszelkie inne operacje przetwarzania są dopuszczalne wyłącznie:
  - za zgodą osoby, której dane dotyczą;
  - w celu ustalenia, dochodzenia lub obrony roszczeń;
  - w celu ochrony praw innej osoby fizycznej lub prawnej;
  - z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.
- w razie dokonania ograniczenia przetwarzania – obowiązek poinformowania o ograniczeniu danych każdego odbiorcy, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku (art. 19 RODO).

Sposób realizacji Żądania:

Wyżej wymieniona żądanie musi być realizowane bez jakichkolwiek opłat na rzecz Administratora.
Jeżeli Dane Osobowe są przetwarzane w sposób automatyczny (z wykorzystaniem systemów IT), realizacja Żądania powinna nastąpić przez jego odnotowanie w systemach zapewniające, iż dane będą jedynie przechowywane i nie wykorzystywane w innym celu. Może to nastąpić np. poprzez przeniesienie danych do wyodrębnionego podzbioru (systemu), czasowe zablokowanie danych na stronie internetowej (np. zablokowanie profilu użytkownika) lub w inny sposób zablokowanie dostępu do danych.

Zakres obowiązku poinformowania o ograniczeniu przetwarzania każdego odbiorcy, któremu ujawniono dane osobowe, może zostać ograniczony, jeżeli administrator wykaże, że wymagałoby to niewspółmiernie dużego wysiłku.

Termin realizacja Żądania:
Bez zbędnej zwłoki, nie później jednak niż miesiąc od otrzymania Żądania. W razie potrzeby istnieje możliwość przedłużenia tego terminu do trzech miesięcy, jednakże tylko z uwagi na skomplikowany charakter Żądania lub liczbę żądań (o czym należy poinformować podmiot żądający w terminie miesiąca od otrzymania żądania). Gdy Administrator nie zamierza podjąć działań w związku z Żądaniem, informuje o tym osobę żądającą niezwłocznie, najpóźniej w terminie miesiąca od otrzymania Żądania.

5. PRAWO DO PRZENOSZENIA DANYCH

Podstawa prawna: art. 20 RODO

Treść Żądania:
- żądanie przekazania w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego danych osobowych, które podmiot danych dostarczył Administratorowi;
- żądanie, aby Administrator nie czynił przeszkód w przesłaniu otrzymanych wyżej danych innemu administratorowi przez samą osobę, której dane dotyczą;
- żądanie, aby Dane Osobowe zostały przesłane przez administratorowi bezpośrednio innemu administratorowi (we wskazanym wyżej formacie), o ile jest to technicznie możliwe.

Zakres obowiązku Administratora:
- obowiązek przekazania podmiotowi żądającemu wszelkich danych, które dostarczył on Administratorowi, w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego (np. format XML, JSON, CSV). Chodzi tu o przekazanie danych w takim formacie, aby umożliwić przesłanie danych z jednego środowiska IT do innego (zachodzi więc konieczność przekazania pliku wraz z metadanymi). Obowiązek ten dotyczy jedynie sytuacji, gdy:
  - przetwarzanie odbywa się na podstawie zgody, bądź na podstawie umowy;
  - przetwarzanie odbywa się w sposób zautomatyzowany (obowiązek ten nie dotyczy więc zbiorów papierowych).

  Wskazany obowiązek odnosi się jedynie do danych, które podmiot dostarczył Administratorowi, tj. danych aktywnie i świadomie przekazanych przez osobę, której dane dotyczą (np. poprzez wypełnienie formularza on-line, przesłanie maila), bądź danych zaobserwowanych w związku z korzystaniem z usługi lub urządzenia przez osobę, której dane dotyczą (np. historia wyszukiwania, dane o ruchu, dane lokalizacyjne). Nie dotyczy to natomiast danych wygenerowanych przez samego administratora na podstawie tych „danych pierwotnych" np. wynik oceny dotyczącej

zdrowia, wygenerowany profil użytkownika, ocena zdolności kredytowej lub ryzyka ubezpieczeniowego.

- obowiązek nieczynienia przeszkód w prawie podmiotu danych do przesłania tak otrzymanych danych do innego administratora np. poprzez żądanie opłaty za przesłanie danych, brak zapewnienia odpowiedniego formatu, celowe zamaskowanie zbioru danych;
- obowiązek przesłania przez administratora wskazanych danych – na żądanie podmiotu danych – bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.

Sposób realizacji Żądania:

Wyżej wymieniona żądanie musi być realizowane bez jakichkolwiek opłat na rzecz Administratora.
Dane muszą być przesłane w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego. Nie oznacza to jednak obowiązku Administratora wprowadzania kompatybilnych z innymi administratorami systemów przetwarzania Danych Osobowych. System ten powinien jednak umożliwiać pobranie danych w powszechnie używanym formacie. Obowiązek przekazania danych w tym formacie może być również spełniony przez zautomatyzowane narzędzie umożliwiające pobieranie istotnych danych przez sam podmiot danych.
Obowiązek przesłania danych bezpośrednio innemu administratorowi będzie wyłączony, jeżeli Administrator wykaże, że nie jest to technicznie możliwe (np. używane przez obu administratorów formaty danych nie są kompatybilne). W przypadku przesłania danych innemu administratorowi, Administrator nie ma obowiązku sprawdzania, czy administrator odbierający dane zapewnia wystarczające bezpieczeństwo danych i czy ma podstawy do ich przetwarzania – przesłanie następuje bowiem do administratora wskazanego wprost przez podmiot danych.

Termin realizacja Żądania:

Bez zbędnej zwłoki, nie później jednak niż miesiąc od otrzymania żądania. W razie potrzeby istnieje możliwość przedłużenia tego terminu do trzech miesięcy, jednakże tylko z uwagi na skomplikowany charakter Żądania lub liczbę żądań (o czym należy poinformować podmiot żądający w terminie miesiąca od otrzymania żądania). Gdy Administrator nie zamierza podjąć działań w związku z Żądaniem, informuje o tym osobę żądającą niezwłocznie, najpóźniej w terminie miesiąca od otrzymania Żądania.

6. PRAWO DO SPRZECIWU

Podstawa prawna: art. 21 RODO

Treść Żądania:

- Art. 21 (1) RODO – sprzeciw osoby, której dane dotyczą wobec przetwarzania dotyczących jej Danych Osobowych opartego na art. 6 ust. 1 lit. e) lub f), w tym profilowania na podstawie tych przepisów, tj. przetwarzanie dopuszczalne w sytuacji gdy jest to niezbędne do wykonania zadania

realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi (pkt e)) lub gdy przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez stronę trzecią (pkt f)); żądanie osoba fizyczna składa z przyczyn związanych z jej szczególną sytuacją.

- Art. 21 (2)-(3) RODO – sprzeciw osoby, której dane dotyczą wobec przetwarzania jej Danych Osobowych na potrzeby marketingu bezpośredniego, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim. Żądanie osoby wymaga bezwarunkowej realizacji.
- Art. 21 (6) RODO – jeżeli Dane Osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, osoba, której dane dotyczą, ma prawo wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej Danych Osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

Zakres obowiązku Administratora:

Najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie sprzeciwu oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji.

W przypadku złożenia sprzeciwu, o którym mowa w Art. 21 (1) RODO, Administratorowi nie wolno już przetwarzać tych Danych Osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń. Ciężar dowodowy spoczywa po stronie Administratora.

Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego (Art. 21 (2) RODO), Danych Osobowych nie wolno już przetwarzać do takich celów.

Sposób realizacji Żądania:

Wyżej wymieniona żądanie musi być realizowane bez jakichkolwiek opłat na rzecz Administratora.

W związku z korzystaniem z usług społeczeństwa informacyjnego i bez uszczerbku dla dyrektywy 2002/58/WE osoba, której dane dotyczą, może wykonać prawo do sprzeciwu za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne (w szczególności, gdy przetwarzanie odbywa się przy wykorzystaniu narzędzi online).

Termin realizacja Żądania:

Bez zbędnej zwłoki, nie później jednak niż miesiąc od otrzymania Żądania. W razie potrzeby istnieje możliwość przedłużenia tego terminu do trzech miesięcy, jednakże tylko z uwagi na skomplikowany charakter Żądania lub liczbę żądań (o czym należy poinformować podmiot żądający w terminie miesiąca od otrzymania żądania). Gdy Administrator nie zamierza podjąć działań w związku z Żądaniem, informuje o tym osobę żądającą niezwłocznie, najpóźniej w terminie miesiąca od otrzymania Żądania.

knowit

7. PRAWA ZWIĄZANE Z ZAUTOMATYZOWANYM PODEJMOWANIEM DECYZJI, W TYM PROFILOWANIEM

Podstawa prawna: art. 22 RODO

Treść Żądania:

- sprzeciw osoby, której dane dotyczą wobec podlegania decyzji , która opiera się wyłącznie na zautomatyzowanym przetwarzaniu danych, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.

Zakres obowiązku Administratora:

Administrator nie ma obowiązku uwzględnienia sprzeciwu, jeżeli decyzja oparta na zautomatyzowanym przetwarzaniu danych:

- jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem;
- jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub
- opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

Zautomatyzowane decyzje, o których mowa powyżej, nie mogą opierać się na szczególnych kategoriach Danych Osobowych, o których mowa w art. 9 ust. 1 RODO, chyba że zastosowanie ma art. 9 ust. 2 lit. a) lub g) RODO i istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.

Sposób realizacji Żądania:

Administrator wdraża właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji.

Termin realizacja Żądania:

Bez zbędnej zwłoki, nie później jednak niż miesiąc od otrzymania Żądania. W razie potrzeby istnieje możliwość przedłużenia tego terminu do trzech miesięcy, jednakże tylko z uwagi na skomplikowany charakter Żądania lub liczbę żądań (o czym należy poinformować podmiot żądający w terminie miesiąca od otrzymania żądania). Gdy Administrator nie zamierza podjąć działań w związku z Żądaniem, informuje o tym osobę żądającą niezwłocznie, najpóźniej w terminie miesiąca od otrzymania Żądania.

Załącznik nr 2
do Polityki Ochrony Danych Osobowych z dnia 10 lutego 2022 r.

PROCEDURA
OBSŁUGI NARUSZEŃ OCHRONY DANYCH OSOBOWYCH
W KNOWIT POLAND SP. Z O.O.

1 stycznia 2022 r.

Knowit Poland sp. z o.o.
ul. Hrubieszowska 2
01-209 Warszawa
NIP: 951 178 99 96

Ph +48 22 355 21 70
Fax +48 22 355 21 71
www.knowit.eu

KRS 0000036076
Sąd Rejonowy dla m.st. Warszawy
XII Wydział Gospodarczy KRS
Kapitał zakładowy: 1 251 200 PLN

PROCEDURA
OBSŁUGI NARUSZEŃ OCHRONY DANYCH OSOBOWYCH
W KNOWIT POLAND SP. Z O.O.

10. DEFINICJE

Na potrzeby Procedury obsługi naruszeń ochrony Danych Osobowych przyjmuje się następujące definicje:

(14) „**Administrator**" – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Administratorem jest Knowit PL. W przypadku, gdy Knowit działa na zlecenie klienta, Administratorem jest klient, a Knowit występuje w roli podmiotu przetwarzającego. W określonych przypadkach Knowit Pl działa jako dalszy podmiot przetwarzający dane;

(15) „**Knowit PL**" – Knowit Poland sp. z o.o. z siedzibą w Warszawie, ul. Hrubieszowska 2, 01-209 Warszawa, wpisana do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie XII Wydział Gospodarczy pod numerem KRS: 0000036076, NIP: 951-17-89-996; REGON: 01284093700000, kapitał zakładowy: 1.251.200,00 zł;

(16) „**Dane Osobowe**" lub „**dane**" – oznaczają 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, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologoczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

(17) „**Koordynator Ochrony Danych Osobowych**" lub „**KODO**" – ustanowiona w Knowit PL funkcja niezależnego eksperta z zakresu ochrony danych osobowych nadzorującego przetwarzanie Danych Osobowych w Knowit PL;

(18) „**Naruszenie**" – 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;

(19) „**Personel**" – oznacza Pracowników i Współpracowników Knowit PL;

(20) „**Pracownik**" – oznacza osobę związaną stosunkiem pracy z Knowit PL;

(21) „**Prezes Urzędu Ochrony Danych Osobowych**" lub „**PUODO**" – oznacza właściwy organ administracji publicznej odpowiedzialny za realizację zadań w zakresie ochrony Danych Osobowych;

(22) „**Procedura Obsługi Naruszeń**", „**Procedura**" lub „**PON**" – oznacza niniejszą procedurę postępowania w przypadku naruszenia ochrony Danych Osobowych obowiązującą w Knowit PL;

(23) „**Rejestr Naruszeń Ochrony Danych Osobowych**" lub „**Rejestr**" – oznacza rejestr przypadków, w których doszło do Naruszenia ochrony Danych Osobowych w Knowit PL;

(24) „**RODO**" – oznacza 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 (ogólne rozporządzenie o ochronie danych) (Dz.U. UE. L. z 2016 r. Nr 119, str. 1);

(25) „**Współpracownik**" – oznacza osobę związaną z Knowit PL stosunkiem zlecenia lub innej umowy cywilnoprawnej, a także praktykanta i stażystę;

(26) „**Zawiadomienie PUODO**" – oznacza dopełnienie obowiązku wynikającego z Procedury Obsługi Naruszeń oraz przepisów prawa przez złożenie zawiadomienia do Prezesa Urzędu Ochrony Danych Osobowych o stwierdzeniu Naruszenia zgodnie z Punktem 6 poniżej.

(27) „**Zawiadomienie PD**" – oznacza dopełnienie obowiązku wynikającego z Procedury Obsługi Naruszeń oraz przepisów prawa w razie stwierdzenia Naruszenia przez zawiadomienie podmiotu danych, którego dotyczy Naruszenie (osoby, której dane dotyczą), o takim Naruszeniu zgodnie z Punktem 7 poniżej.

11. CEL I ZAKRES PROCEDURY

3. W celu zapewnienia kontroli nad przetwarzaniem Danych Osobowych, w szczególności w sytuacjach związanych z Naruszeniem ochrony Danych Osobowych, a także efektywnego działania w celu zminimalizowania ewentualnych ryzyk związanych z Naruszeniem i sprostania wymogom RODO związanym z dokonywaniem zawiadomień o Naruszeniu, przyjmuje się Procedurę Obsługi Naruszeń.
4. Procedura Obsługi Naruszeń reguluje:
   (3) zasady postępowania w przypadku Naruszenia,
   (4) zasady prowadzenia Rejestru i dokumentacji przypadków Naruszeń,
   (5) tryb zgłaszania Naruszeń PUODO i przypadki, w których zgłoszenie nie jest wymagane,
   (6) tryb zawiadamiania osoby, której dane dotyczą, o Naruszeniu i przypadki, w których zawiadomienie nie jest wymagane.

12. OBOWIĄZKI PERSONELU ZWIĄZANE Z OBSŁUGĄ NARUSZEŃ

7. Każdy Pracownik i Współpracownik obowiązany jest do zapoznania się i stosowania Procedury Obsługi Naruszeń.
8. Każdy Pracownik i Współpracownik, pozyskawszy wiadomość o Naruszeniu, ma obowiązek natychmiast zawiadomić o tym fakcie ustnie lub w formie wiadomości e-mail swojego bezpośredniego przełożonego oraz KODO. Zawiadomienie KODO należy przesłać na następujący adres e-mail: dataprotection@knowitgroup.com .
9. Naruszenia, które należy zgłosić bezpośredniemu przełożonemu oraz KODO obejmują w szczególności następujące przypadki:
   (1) zgubienie lub kradzież nośnika/urządzenia zawierającego Dane Osobowe;

(2) zgubienie, kradzież lub pozostawienie w niezabezpieczonej lokalizacji dokumentacji papierowej zawierającej Dane Osobowe;
(3) nieuprawnione uzyskanie dostępu do informacji;
(4) nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń;
(5) złośliwe oprogramowanie ingerujące w poufność, integralność i dostępność Danych Osobowych;
(6) uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (*phishing*);
(7) nieprawidłowa anonimizacja Danych Osobowych w dokumencie;
(8) nieprawidłowe usunięcie/zniszczenie Danych Osobowych z nośnika/urządzenia elektronicznego;
(9) niezamierzona publikacja materiałów zawierających Dane Osobowe;
(10) Dane Osobowe wysłane do niewłaściwego odbiorcy;
(11) ujawnienie Danych Osobowych osobie nieuprawnionej do ich posiadania.

10. Zawiadomienie, o którym mowa w Punkcie 3.2 powyżej, powinno w miarę możliwości opisywać charakter i skalę Naruszenia, liczbę osób, których danych dotyczy Naruszenie, a także zastosowanie lub proponowane środki w celu zaradzenia Naruszeniu.
11. Zawiadomienie, o którym mowa w Punkcie 3.2 powyżej, należy złożyć najpóźniej w ciągu 1 (jednej) godziny od chwili pozyskania wiadomości o Naruszeniu.
12. Każdy Pracownik i Współpracownik obowiązany jest do udzielania przełożonemu i KODO wszelkich wyjaśnień związanych ze stwierdzonym Naruszeniem, w szczególności poprzez zapewnienie dostępu do informacji, materiałów, dokumentów lub narzędzi informatycznych. Pracownik i Współpracownik obowiązany jest udzielić wyjaśnień niezwłocznie, nie później jednak niż w terminie 4 (czterech) godzin od stwierdzenia Naruszenia lub podejrzenia Naruszenia.

13. OBOWIĄZKI KODO ZWIĄZANE Z OBSŁUGĄ NARUSZEŃ

2. KODO:
(6) nadzoruje przestrzeganie w Knowit PL przepisów o ochronie Danych Osobowych, w tym związanych z postępowaniem w przypadku zaistnienia Naruszenia;
(7) na bieżąco monitoruje zawiadomienia o Naruszeniach pod adresem e-mail, o którym mowa w Punkcie 3.2 powyżej;
(8) prowadzi działania w celu ustalenia przyczyn, skali i skutków Naruszenia, a w szczególności liczby osób, których Danych Osobowych dotyczy Naruszenie;
(9) rekomenduje Zarządowi Knowit PL środki zaradcze mające na celu wyeliminowanie lub złagodzenie skutków Naruszenia;
(10) koordynuje zastosowanie zaakceptowanych przez Zarząd Knowit PL środków zaradczych zmierzających do wyeliminowania, a gdy nie jest to możliwe, do złagodzenia skutków Naruszenia;

(11) koordynuje działania w Knowit PL związane z oceną, czy jest prawdopodobne, by Naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych oraz czy to ryzyko jest wysokie;
(12) koordynuje działania w Knowit PL w celu przygotowania Zawiadomienia PUODO i Zawiadomienia PD oraz redaguje projekt Zawiadomienia PUODO i Zawiadomienia PD, który przedkłada Zarządowi Knowit PL do akceptacji;
(13) w imieniu Zarządu Knowit PL dokonuje Zawiadomienia PUODO;
(14) w imieniu Zarządu Knowit PL dokonuje Zawiadomień PD;
(15) prowadzi Rejestr Naruszeń Ochrony Danych Osobowych;
(16) dokumentuje wszelkie przypadki Naruszeń, w tym okoliczności powstania Naruszeń, ich skutki oraz podjęte działania zaradcze;
(17) koordynuje prace związane z wprowadzeniem środków organizacyjnych i bezpieczeństwa w celu zminimalizowania ryzyka wystąpienia Naruszeń w przyszłości.

14. REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

4. KODO prowadzi Rejestr Naruszeń Ochrony Danych Osobowych w formie elektronicznej i dokonuje w nim wpisów w razie stwierdzenia Naruszenia.
5. KODO decyduje o umieszczeniu zawiadomienia, o którym mowa w Punkcie 3.2 powyżej, w Rejestrze. Jeżeli KODO postanowi o niewpisaniu zawiadomienia do Rejestru w związku z tym, iż zawiadomienie nie dotyczy sytuacji Naruszenia, obowiązany jest sporządzić notatkę ze swoich ustaleń.
6. Wpis do Rejestru powinien zawierać:
   (6) opis charakteru, skali i skutków Naruszenia, a w szczególności liczbę osób, których Danych Osobowych dotyczy Naruszenie;
   (7) informacje o podjętych i rekomendowanych środkach zaradczych mających na celu wyeliminowanie lub złagodzenie skutków Naruszenia;
   (8) wzmiankę o poinformowaniu PUODO o stwierdzonym Naruszeniu lub braku konieczności powiadomienia;
   (9) wzmiankę o poinformowaniu osoby, której dane dotyczą o stwierdzonym Naruszeniu lub braku konieczności powiadomienia.

15. ZAWIADOMIENIE PUODO

7. W przypadku stwierdzenia Naruszenia ochrony Danych Osobowych administrowanych przez Knowit PL, Knowit PL bez zbędnej zwłoki, nie później niż w terminie 72 godzin od stwierdzenia Naruszenia, zgłasza Naruszenie PUODO, chyba że jest mało prawdopodobne, by Naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. W przypadku gdy do Naruszenia dojdzie w związku z przetwarzaniem przez Knowit PL Danych Osobowych w imieniu innego administratora danych lub gdy Knowit będzie działał jako dalszy podmiot przetwarzający, należy postępować zgodnie z Punktem 8 Procedury.

8. Analizując ryzyko naruszenia praw lub wolności osób fizycznych, o którym mowa w Punkcie 6.1 powyżej, Knowit PL bierze pod uwagę w szczególności charakter, skalę i możliwe skutki Naruszenia, a także liczbę osób, których Danych Osobowych dotyczyło Naruszenie.
9. Analizę w zakresie spełnienia przesłanek do dokonania Zawiadomienia PUODO przeprowadza zespół składający się z przedstawiciela działu IT, właściciela procesu, w którym doszło do Naruszenia, KODO oraz przedstawiciela kadry zarządzającej. Wynik analizy zostaje opisany w Rejestrze. W Załączniku nr 2 do niniejszej Procedury zawarto wskazówki interpretacyjne dotyczące oceny Naruszenia, w tym pod kątem konieczności dokonania Zawiadomienia PUODO.
10. Jeżeli na podstawie analizy, o której mowa w Punkcie 6.2 i 6.3 powyżej, Knowit PL stwierdzi, iż nie zostały spełnione przesłanki do dokonania Zawiadomienia PUODO, informacja dotycząca Naruszenia i wyników analizy zostaje umieszczona w Rejestrze z adnotacją o braku konieczności dokonania Zawiadomienia PUODO.
11. Zawiadomienie PUODO, o którym mowa w Punkcie 6.1 powyżej, powinno:
    (1) zawierać nazwę oraz dane kontaktowe Knowit PL oraz KODO;
    (2) określać datę i godzinę zaistnienia Naruszenia, jeżeli jest to możliwe;
    (3) opisywać okoliczności zaistnienia i charakter Naruszenia ochrony Danych Osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów Danych Osobowych, których dotyczy Naruszenie;
    (4) opisywać możliwe konsekwencje Naruszenia ochrony Danych Osobowych;
    (5) opisywać środki zastosowane lub proponowane przez Administratora w celu zaradzenia Naruszeniu ochrony Danych Osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
12. Zgłoszenie powinno zostać dokonane na formularzu oraz zgodnie z wytycznymi PUODO udostępnionymi na urzędowej stronie PUODO https://uodo.gov.pl/pl/134/233 lub aktualnie obowiązującej.
13. Jeżeli Knowit PL nie ma możliwości złożyć kompletnego zawiadomienia PUODO zgodnie z wymagania określonymi w Punkcie 6.5 powyżej, powinien, w miarę możliwości, przedstawić wstępne zawiadomienie z informacją o podjętych działaniach w celu uzupełnienia informacji, a także wiadomością o przewidywanym terminie uzupełnienia zawiadomienia.
14. Do zgłoszenia przekazanego PUODO po upływie 72 godzin od stwierdzenia Naruszenia Knowit PL dołącza wyjaśnienie przyczyn opóźnienia.
15. Jeżeli Naruszenie dotyczy danych osób w różnych krajach UE, PUODO może być, ale nie musi być wiodącym (czyli właściwym dla administratora lub podmiotu przetwarzającego) organem nadzorczym. W przypadku transgranicznego naruszenia Danych Osobowych administrator powinien dokonać analizy, czy wiodącym organem nadzoru w odniesieniu do czynności przetwarzania, które zostały objęte naruszeniem jest PUODO, czy też inny europejski Organ Nadzorczy.

16. ZAWIADOMIENIE PODMIOTU DANYCH (ZAWIADOMIENIE PD)

8. Jeżeli stwierdzone Naruszenie ochrony Danych Osobowych administrowanych przez Knowit PL może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Knowit PL bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim Naruszeniu, nie później jednak niż w terminie 3 (trzech) dni od ustalenia, że Naruszenie powoduje wysokie ryzyko dla praw lub wolności tej osoby. W przypadku gdy do Naruszenia dojdzie w związku z przetwarzaniem przez Knowit PL Danych Osobowych w imieniu innego administratora danych lub gdy Knowit PL będzie działał jako dalszy podmiot przetwarzający, należy postępować zgodnie z Punktem 8 Procedury.
9. Analizę w zakresie spełanienia przesłanek do dokonania Zawiadomienia PD przeprowadza zespół składający się z przedstawiciela działu IT, właściciela procesu, w którym doszło do Naruszenia, KODO oraz przedstawiciela kadry zarządzającej. Wynik analizy zostaje wskazany w Rejestrze.
10. Zawiadomienie PD opisuje charakter Naruszenia ochrony Danych Osobowych jasnym i prostym językiem oraz zawiera:
    (1) nazwę oraz dane kontaktowe Knowit PL oraz KODO z adnotacją o możliwości uzyskania dalszych informacji;
    (2) opis możliwych konsekwencji Naruszenia ochrony Danych Osobowych;
    (3) opis środków zastosowanych lub proponowanych w celu zaradzenia Naruszeniu, w tym w stosownych przypadkach środki w celu zminimalizowania ewentualnych negatywnych skutków Naruszenia.
11. Jeżeli Knowit PL nie dokonał Zawiadomienia PD zgodnie z Punktem 7.1 powyżej, a PUODO zażądał dokonania takiego zawiadomienia, Knowit PL bez zbędnej zwłoki, nie później jednak niż w terminie 3 (trzech) dni od doręczenia stanowiska PUODO, dokonuje Zawiadomienia PD zgodnie z żądaniem PUODO.
12. Zawiadomienie PD nie jest wymagane jeżeli:
    (1) wdrożono odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do Danych Osobowych, których dotyczy Naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych Danych Osobowych;
    (2) zastosowano następczo środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o czym mowa w Punkcie 7.1 powyżej;
    (3) dokonanie Zawiadomienia PD wymagałoby niewspółmiernie dużego wysiłku.
13. W przypadku, o którym mowa w Punkcie 7.5 ppkt (3) powyżej, Knowit PL zobowiązany jest do wydania publicznego komunikatu lub wykorzystania środka równoważnego, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób o stwierdzonym Naruszeniu.

17. ZGŁOSZENIA NARUSZEŃ DO ADMINISTRTATORÓW DANYCH LUB PODMIOTÓW PRZETWARZAJĄCYCH

4. W przypadku gdy do Naruszenia dojdzie w związku z przetwarzaniem przez Knowit PL Danych Osobowych w imieniu innego administratora danych lub gdy Knowit PL będzie działał jako dalszy

podmiot przetwarzający, niezwłocznie po stwierdzeniu Naruszenia Knowit PL zawiadomi takiego administratora lub podmiot przetwarzający, na rzecz którego działa.

5. W opisanym procesie zastosowanie mają tryb i terminy zawiadomień przewidziane w umowach powierzenia przetwarzania Danych Osobowych zawartych przez Knowit PL z kontrahentami będącymi administratorami lub podmiotami przetwarzającymi.
6. Uwzględniając charakter przetwarzania oraz dostępne Knowit PL informacje, Knowit PL będzie wspierał administratora danych lub podmiot przetwarzający w zakresie obowiązków, które podmioty te posiadają dotyczących zawiadamiania PUODO i podmiotów danych o Naruszeniach.

18. POSTANOWIENIA KOŃCOWE

3. Integralną część niniejszej Procedury stanowi załącznik: „*Wskazówki dotyczące oceny charakteru Naruszenia i związanych z nim ryzyk*."
4. Procedura wchodzi w życie z dniem 1 stycznia 2022 r.

knowit

Załącznik

Wskazówki dotyczące oceny charakteru Naruszenia i związanych z nim ryzyk

1. Za Naruszenie, które wymaga Zawiadomienia PUODO może być uznane w szczególności:
   (1) utrata poufności lub integralności Danych Osobowych uniemożliwiająca wykonywanie obowiązków Administratora lub Podmiotu Przetwarzającego;
   (2) wyciek bazy danych zawierającej informacje identyfikujące osobę i umożliwiające przejęcie jej tożsamości lub wykonanie transakcji (powiązanie takich danych jak, np.: imię i nazwisko, adres zameldowania, dane teleadresowe, numer PESEL, numer telefonu, adres konta poczty elektronicznej, dane dokumentu tożsamości, które umożliwi zidentyfikowanie osoby fizycznej);
   (3) wyciek bazy zawierającej Dane Osobowe lub narzędzia służące do uwierzytelniania transakcji płatniczych lub korzystania z elektronicznych kanałów dostępu;
   (4) wysłanie korespondencji zawierającej Dane Osobowe do osoby nieuprawnionej (w formie papierowej lub elektronicznej);
   (5) kradzież lub zgubienie dokumentów papierowych zawierających Dane Osobowe;
   (6) kradzież lub zgubienie urządzeń przenośnych, mobilnych oraz elektronicznych nośników danych (np. laptopów, tabletów, smartfonów, pendrive'ów) zawierających niezabezpieczone (poprzez kryptograficzne środki ochrony, np. szyfrowanie) Dane Osobowe.
2. Naruszenie nie wymaga Zawiadomienia PUODO, jeżeli jest mało prawdopodobne, by skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Za Naruszenie, które nie wymaga Zawiadomienia PUODO może być uznane w szczególności:
   (1) wyciek danych, które nie umożliwiają identyfikacji osoby fizycznej, przejęcia jej tożsamości lub wykonania transakcji (np. baza danych po pseudonimizacji lub część bazy zawierająca tylko nazwy ulic, nazwy miast lub kody pocztowe);
   (2) wyciek Danych Osobowych zabezpieczonych z zastosowaniem środków kryptograficznej ochrony (np. z wykorzystaniem szyfrowania lub pseudonimizacji), z zastrzeżeniem, że nie doszło do jednoczesnego skompromitowania kluczy kryptograficznych używanych do ochrony Danych Osobowych (np. klucza PGP);
   (3) wyciek Danych Osobowych lub narzędzia służącego do uwierzytelniania transakcji płatniczych lub korzystania z elektronicznych kanałów dostępu zabezpieczonych z zastosowaniem kryptograficznych środków ochrony (np. z wykorzystaniem szyfrowania lub pseudonimizacji), z zastrzeżeniem, że nie doszło do jednoczesnego skompromitowania kluczy kryptograficznych używanych do ochrony Danych Osobowych (np. klucza PGP);
   (4) wysłanie Danych Osobowych w korespondencji elektronicznej do osoby nieuprawnionej z zastosowaniem kryptograficznych środków ochrony (zaszyfrowanych, zahasłowanych) bez jednoczesnego dostępu do narzędzi deszyfrujących i haseł;
   (5) kradzież lub zagubienie urządzeń przenośnych, mobilnych oraz elektronicznych nośników danych zawierających Dane Osobowe zabezpieczonych z zastosowaniem organizacyjnych,

technicznych lub kryptograficznych środków ochrony (np. szyfrowanie, bezpieczne hasła, możliwość zdalnego czyszczenia danych z urządzenia mobilnego);

(6) ujawnienie informacji prawnie chronionych osobie trzeciej, jeśli do ich ujawnienia doszło z winy osoby, której dane dotyczą, w tym udostępnienie danych do logowania, umożliwienie zapoznania się z wiadomościami z poczty elektronicznej lub wiadomościami SMS.

3. Możliwe negatywne konsekwencje dla osoby, której dane dotyczą związane z Naruszeniem, które mogą mieć zasadniczy wpływ na ocenę charakteru Naruszenia:
   (1) utrata kontroli nad własnymi Danymi Osobowymi;
   (2) ograniczenie możliwości realizowania praw z art. 15-22 RODO;
   (3) ograniczenie możliwości realizowania innych uprawnień osób, których dane dotyczą, niż określone w pkt. (2) powyżej;
   (4) dyskryminacja;
   (5) kradzież lub sfałszowanie tożsamości;
   (6) strata finansowa;
   (7) naruszenie dobrego imienia;
   (8) utrata poufności danych osobowych chronionych tajemnicą zawodową;
   (9) nieuprawnione odwrócenie pseudonimizacji (możliwość ponownego połączenia informacji z dwóch źródeł umożliwiająca identyfikację osoby).