Polityka prywatności oraz ochrony danych osobowych strony www.turystykakika.pl i stron współpracujących

1. Niniejszy dokument zatytułowany „Polityka ochrony danych osobowych" (dalej jako: **Polityka**) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w firmie Domki letniskowe „Kika" Wojciech Stępień adres ul. Młyńska 28 76-034 Srabinowo.
   Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu Rozporządzenia Parlamentu Europejskiego i Rady(UE) 2016/679 z 27.04.2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1) – dalej jako RODO.

2. Polityka zawiera:
   a) opis zasad ochrony danych osobowych, które obowiązują w naszej firmie;
   b) odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach).

3. Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest Właściciel Firmy Domki Letniskowe „Kika" Wojciech Stępień

4. Za nadzór i monitorowanie przestrzegania i stosowanie niniejszej Polityki odpowiada Właściciel ww firmy.

5. Skróty i definicje:
   a) Polityka – oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu;
   b) **RODO** – oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1);
   c) **Dane** – oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu;
   d) **Dane szczególnych kategorii** – oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej;
   e) **Dane karne** – oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa;
   f) **Dane dzieci** – oznaczają dane osób poniżej 16 roku życia;
   g) **Osoba** – oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu;
   h) **Podmiot przetwarzający** – oznacza organizację lub osobę, której Spółka powierzyła przetwarzanie danych osobowych (np. usługodawca IT, zewnętrzna księgowość);
   i) **Profilowanie** – oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
   j) **Eksport danych** – oznacza przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej;

k) **IOD lub Inspektor** – oznacza Inspektora Ochrony Danych Osobowych;
l) **RCPD lub Rejestr** – oznacza Rejestr Czynności Przetwarzania Danych;
m) **Spółka** – oznacza spółkę e-turysta spółka z ograniczoną odpowiedzialnością spółka komandytowa z siedzibą w Krakowie przy ulicy Albatrosów 1, 30-716 Kraków, posiadającą numer NIP 679-30-26-999, posiadającą numer KRS 0000605523.

6. Ochrona danych osobowych w naszej firmie - zasady ogólne

8.1. Filary ochrony danych osobowych w firmie:
a) **Legalność** – Firma dba o ochronę prywatności i przetwarza dane osobowe zgodnie z prawem;
b) **Bezpieczeństwo** – Firma zapewnia odpowiedni poziom bezpieczeństwa danych osobowych, podejmując stale działania w tym zakresie;
c) **Prawa jednostki** – Firma umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje;
d) **Rozliczalność** – Firma dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili mieć możliwość wykazać zgodność przetwarzania.

8.2. Zasady ochrony danych osobowych.
Firma przetwarza dane osobowe z poszanowaniem następujących zasad:
a) w oparciu o podstawę prawną i zgodnie z prawem (**legalizm**);
b) rzetelnie i uczciwie (**rzetelność**);
c) w sposób przejrzysty dla osoby, której dane osobowe dotyczą (**transparentność**);
d) w konkretnych celach i nie na „zapas” (**minimalizacja**);
e) nie więcej niż potrzeba (**adekwatność**);
f) z dbałością o prawidłowość danych osobowych (**prawidłowość**);
g) nie dłużej niż potrzeba (**czasowość**);
h) zapewniając odpowiednie bezpieczeństwo danych osobowych (**bezpieczeństwo**).

8.3. System ochrony danych osobowych.
System ochrony danych osobowych w firmie Domki letniskowe „Kika” składa się z następujących elementów:
1) **Inwentaryzacja danych osobowych** – Firma dokonuje identyfikacji zasobów danych osobowych w Firmie oraz identyfikacji sposobów wykorzystania danych osobowych, w tym:
a) przypadków przetwarzania danych szczególnych kategorii i danych karnych;
b) przypadków przetwarzania danych osobowych, których firma nie identyfikuje;
c) przypadków przetwarzania danych osobowych dzieci;
d) profilowania;
e) współadministrowania danymi osobowymi.
2) **Rejestr** – Firma opracowuje, prowadzi i utrzymuje Rejestr. Rejestr jest narzędziem rozliczenia zgodności z ochroną danych osobowych w firmie.
3) **Podstawy prawne** – Firma zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych osobowych i rejestruje je w Rejestrze, w tym:
a) utrzymuje system zarządzania zgodami na przetwarzanie danych osobowych i komunikację na odległość;
b) inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy firma przetwarza dane osobowe na podstawie prawnie uzasadnionego interesu firmy.
4) **Obsługa praw jednostki** – Firma spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, a tym:
a) **obowiązki informacyjne** – Firma przekazuje osobom prawem wymagane informacje przy zbieraniu danych osobowych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków;

b) **możliwość wykonania żądań** – Firma weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających;
c) **obsługa żądań** – Firma zapewnia odpowiednie nadkłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany przez RODO i dokumentowane;
d) **zawiadomienie o naruszeniach** – Firma stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych osobowych.
5) **Minimalizacja** – Firma posiada zasady i metody zarządzania minimalizacją (privacy by default), a w tym:
a) zasady zarządzania adekwatnością danych osobowych;
b) zasady reglamentacji i zarządzania dostępem do danych osobowych;
c) zasady zarządzania okresem przechowywania danych osobowych i weryfikacji dalszej ich przydatności.
6) **Bezpieczeństwo** – Firma zapewnia odpowiedni poziom bezpieczeństwa danych osobowych, w tym:
a) przeprowadza analizy ryzyka dla czynności przetwarzania danych osobowych lub ich kategorii;
b) przeprowadza oceny skutków dla ochrony danych osobowych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;
c) dostosowuje środki ochrony danych osobowych do ustalonego ryzyka;
d) posiada system zarządzania bezpieczeństwem informacji;
e) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych osobowych Urzędowi Ochrony Danych.
7) **Przetwarzający** – Firma posiada zasady doboru przetwarzających dane osobowe na rzecz Spółki, wymogów co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia.
8) **Eksport danych osobowych** – Firma posiada zasady weryfikacji, czy nikt nie przekazuje danych osobowych do państw trzecich (czyli poza Unię Europejską, Norwegię, Liechtenstein oraz Islandię) lub do organizacji międzynarodowych oraz zapewnia zgodnych z prawem warunków takiego przekazywania, jeżeli ma ono miejsce.
9) **Projektowanie prywatności (privacy by design)** – Firma zarządza zmianami wpływającymi na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji w Firmie uwzględniają konieczność oceny wpływu zmiany na ochronę danych osobowych, analizę ryzyka, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych osobowych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.
10) **Przetwarzanie transgraniczne** – Firma posiada zasady weryfikacji, kiedy zachodzą przypadki przetwarzania transgranicznego oraz zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO.

7. Inwentaryzajca

9.1. Dane szczególnej kategorii i dane karne.
Firma nie przetwarza takich danych.

9.2. Dane niezidentyfikowane.
Firma nie gromadzi takich danych

9.3. Współadministrowanie.
Firma identyfikuje przypadki współadministrowania danymi osobowymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami.

8. Rejestr czynności przetwarzania danych.

10.1. Rejestr Czynności Przetwarzania Danych stanowi formę dokumentowania czynności przetwarzania

danych osobowych, pełni rolę mapy przetwarzania danych osobowych w Firmie i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.

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

10.3. Rejestr Czynności Przetwarzania Danych jest jednym z podstawowych narzędzi umożliwiających Firmie rozliczanie większości obowiązków ochrony danych osobowych.

10.4. W Rejestrze Czynności Przetwarzania Danych dla każdej czynności przetwarzania danych osobowych, którą Firma uznała za odrębną dla potrzeb Rejestru, Firma odnotowuje co najmniej:
a) nazwę czynności;
b) cel przetwarzania;
c) opis kategorii osób;
d) opis kategorii danych;
e) podstawę prawną przetwarzania danych osobowych, wraz z wyszczególnieniem kategorii uzasadnionego interesu Firmy jeżeli taką podstawą jest uzasadniony interes Spółki;
f) sposób zbierania danych osobowych;
g) opis kategorii odbiorców danych osobowych (w tym przetwarzających);
h) informację o przekazywaniu danych osobowych poza Unię Europejską/Europejski Obszar Gospodarczy;
i) ogólny opis technicznych i organizacyjnych środków ochrony danych osobowych.

10.5. Wzór Rejestru Czynności Przetwarzania Danych stanowi Załącznik nr 1 do niniejszej Polityki. Przedmiotowy wzór zawiera także kolumny nieobowiązkowe. W kolumnach nieobowiązkowych Spółka rejestruje informację w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść Rejestru ułatwia zarządzanie zgodnością ochrony danych osobowych i rozliczenie się z niej.

9. Podstawy przetwarzania

11.1. Spółka dokumentuje w Rejestrze Czynności Przetwarzania Danych podstawy prawne przetwarzania danych osobowych dla poszczególnych czynności przetwarzania.

11.2. Wskazując w dokumentach ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel Firmy), Spółka dookreśla podstawę w precyzyjny i czytelny sposób, gdy jest to potrzebne. Przykładowo dla zgody – wskazując jej zakres, gdy podstawą jest prawo – wskazując konkretny przepis i inne dokumenty, np. umowę, porozumienie administracyjne, żywotne interesy – wskazując kategorie zdarzeń, w których się zmaterializują, uzasadniony cel – wskazując konkretny cel, np. marketing własny, dochodzenie roszczeń.

11.3. Firma wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych osobowych, w konkretnym celu, zgody na komunikację na odległość (e-mail, telefon, SMS itp.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).

11.4. Kierownik komórki organizacyjnej Firma (jej reprezentant) ma obowiązek znać podstawy prawne, na jakich komórka przez niego kierowana dokonuje konkretnych czynności przetwarzania danych osobowych. Jeżeli podstawą jest uzasadniony interes Firmy , właściciel ma obowiązek znać konkretny realizowany przetwarzaniem interes Firmy.

10. Sposób obsługi praw jednostki i obowiązków informacyjnych

12.1. Firma dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane osobowe przetwarza.

12.2. Firma ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczanie na stronie internetowej Firmy informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich w Firmie, w tym wymaganiach dotyczących identyfikacji, metodach kontaktu z Firmąw tym celu, ewentualnym cenniku żądań „dodatkowych" itp.

12.3. Firma dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.

12.4. Firma wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.

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

12.6. Firma dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

11. Obowiązki informacyjne

13.1. Firma określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.

13.2. Firma informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenia żądania tej osoby.

13.3. Firma informuje osobę o przetwarzaniu jej danych osobowych, przy pozyskiwaniu danych od tej osoby.

13.4. Firma informuje osobę o przetwarzaniu jej danych osobowych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej.

13.5. Firma określa sposób informowania osób o przetwarzaniu danych osobowych nieidentyfikowanych, tam, gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym).

13.6. Firma informuje osobę o planowanej zmianie celu przetwarzania danych osobowych.

13.7. Firma informuje osobę przed uchyleniem ograniczenia przetwarzania danych osobowych.

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

13.9. Firma informuje osobę o prawie sprzeciwu względem przetwarzania danych osobowych najpóźniej przy pierwszym kontakcie z tą osobą.

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

12. Żądania osób

14.1. Nieprzetwarzanie – Firma informuje osobę o tym, że nie przetwarza danych osobowych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.

14.2. Odmowa – Firma informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia jej żądania i o prawach osoby z tym związanych.

14.3. Dostęp do danych – na żądanie osoby dotyczące dostępu do danych osobowych jej dotyczących Firma informuje tę osobę, czy przetwarza jej dane osobowe oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych osobowych), a także udziela osobie dostępu do danych osobowych jej dotyczących. Dostęp do danych osobowych może być zrealizowany poprzez wydanie kopii danych osobowych, z zastrzeżeniem, że kopii danych osobowych wydanej w wykonaniu prawa dostępu do danych osobowych Spółka nie uzna za pierwszą nieodpłatną kopię danych osobowych dla potrzeb opłat za kopie danych osobowych.

14.4. Kopie danych osobowych – na żądanie osoby Spółka wydaje kopie danych osobowych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Firma wprowadza i utrzymuje cennik kopii danych osobowych, zgodnie z którym pobiera opłaty za kolejne kopie danych. Cena kopii danych osobowych skalkulowana jest na podstawie oszacowanego jednostkowego koszu obsługi żądania wydania kopii danych osobowych.

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

14.6. Uzupełnienie danych osobowych – Firma uzupełnia i aktualizuje dane osobowe na żądanie osoby. Spółka ma prawo odmówić uzupełnienia danych osobowych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. Firmanie musi przetwarzać danych osobowych, które są Firma zbędne). Firma może polegać na oświadczeniu osoby co do uzupełniania danych osobowych, chyba że będzie to niewystarczające w świetle przyjętych przez Firmę procedur (np. co do pozyskiwania takich danych osobowych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

14.7. Usunięcie danych osobowych – na żądanie osoby Firma usuwa dane osobowe, gdy:
a) dane osobowe nie są niezbędne do celów, w których zostały zebrane, ani przetwarzane w innych zgodnych z prawem celach;
b) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania;
c) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych osobowych;
d) dane osobowe były przetwarzane niezgodnie z prawem;
e) konieczność usunięcia danych osobowych wynika z obowiązku prawnego;
f) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. profil dziecka na portalu społecznościowym, udział w konkursie na stronie internetowej).
Firma określa sposób obsługi prawa do usunięcia danych osobowych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych osobowych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17 ust. 3 RODO.
Jeżeli dane osobowe podlegające usunięciu zostały upublicznione przez Firmę, Firma podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe o potrzebie usunięcia danych i dostępu do nich.

W przypadku usunięcia danych osobowych Firma informuje osobę o odbiorcach danych, na żądanie tej osoby.

14.8. Ograniczenie przetwarzania danych osobowych – Firma dokonuje ograniczenia przetwarzania danych osobowych na żądanie osoby, gdy:
a) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość;
b) przetwarzanie jest niezgodne z prawem, a osoba, której dane osobowe dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
c) Firma nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
d) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Firmy zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.
W trakcie ograniczenia przetwarzania danych osobowych Firma przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane osobowe dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.
Firma informuje osobę przed uchyleniem ograniczenia przetwarzania danych osobowych.
W przypadku ograniczenia przetwarzania danych osobowych Firma informuje osobę o odbiorcach danych, na żądanie osoby.

14.10. Przenoszenie danych osobowych – na żądanie osoby Spółka wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Firma, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawiązanej w systemach informatycznych Firmy.

14.11. Sprzeciw w szczególnej sytuacji – jeżeli osobo zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych osobowych, a dane przetwarzane są przez Firmę w oparciu o uzasadniony interes Firmy lub o powierzone Firmie zadanie w interesie publicznym, Firma uwzględni sprzeciw, o ile nie zachodzą po stronie Firmy ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

14.12. Sprzeciw względem marketingu bezpośredniego – jeżeli osoba zgłosi sprzeciw względem przetwarzanie jej danych osobowych przez Firmę na potrzeby marketingu bezpośredniego (w tym ewentualnie profilowania), Firmauwzględni sprzeciw i zaprzestanie takiego przetwarzania.

14.13. Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu danych osobowych – jeżeli Firma przetwarza dane osobowe w sposób automatyczny, w tym w szczególności profiluje osoby, i w konsekwencji podejmuje względem osoby decyzje wywołujące skutki prawne lub inaczej istotnie wpływające na osobę, Firma zapewnia możliwość odwołania się do interwencji i decyzji człowieka po stronie Firmy, chyba że taka automatyczna decyzja:
a) jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a Firmą, lub;
b) jest wprost dozwolona przepisami prawa lub;
c) opiera się na wyraźnej zgodzie odwołującej osoby.

13. Minimalizacja
Firma dba o minimalizację przetwarzania danych osobowych pod kątem:
a) adekwatności danych osobowych do celów (ilości danych i zakresu przetwarzania);
b) dostępu do danych osobowych;
c) czasu przechowywania danych.

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

15.2. Minimalizacja dostępu.
Firma stosuje ograniczenia dostępu do danych osobowych: prawne (zobowiązania do poufności, zakresy upoważnień), fizyczne (strefy dostępu, zamykanie pomieszczeń) i logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe).
Firma stosuje kontrolę dostępu fizycznego.
Firma dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób oraz zmianach podmiotów przetwarzających.
Firma dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.
Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w procedurach bezpieczeństwa fizycznego i bezpieczeństwa informacji Firmy.

14. Bezpieczeństwo danych osobowych
Firma zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Firma.

16.1. Analiza ryzyka i adekwatności środków bezpieczeństwa.
Firma przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych.
W tym celu:
1) Firma zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania – wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.
2) Firma kategoryzuje dane osobowe oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.
3) Firma przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych osobowych lub ich kategorii. Firma analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych, uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnych prawdopodobieństwie wystąpienia i wadze zagrożenia.
4) Firma ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrożenia. W tym Firma ustala przydatność i stosuje takie środki i podejście, jak:
a) pseudonimizacja;
b) szyfrowanie danych osobowych;
c) inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności dostępności i odporności systemów i usług przetwarzania;
d) 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.

16.2. Oceny skutków dla ochrony danych osobowych.
Firma dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z zasadą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.
16.3. Środki bezpieczeństwa danych osobowych.
Firma stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków

bezpieczeństwa oraz ocen skutków dla ochrony danych.

16.4. Zgłoszenia naruszeń.
Firma stosuje procedury pozwalające na identyfikację, ocenę i zgłaszanie zidentyfikowanego naruszenia ochrony danych osobowych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia.

15. Przetwarzający
Firma posiada zasady doboru i weryfikacji przetwarzających dane osobowe na rzecz Firmy opracowane w celu zapewnienia, aby przetwarzający dawali wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa i realizacji praw jednostki i innych obowiązków ochrony danych osobowych spoczywających na Firmie.
Firma przyjęła minimalne wymagania do umowy powierzenia przetwarzania danych osobowych stanowiące Załącznik nr 2 do niniejszej Polityki.
Firma rozlicza przetwarzających z wykorzystania podprzetwarzających, jak też z innych wymagań wynikających z zasad powierzenia danych osobowych.

16. Eksport danych osobowych
Firma rejestruje w Rejestrze przypadki eksportu danych osobowych, czyli przekazywania danych poza Europejski Obszar Gospodarczy (Unia Europejska, Islandia, Liechtenstein i Norwegia).
Aby uniknąć sytuacji nieautoryzowanego eksportu danych osobowych w szczególności w związku z wykorzystaniem publicznie dostępnych usług chmurowych (shadow IT), Firma okresowo weryfikuje zachowania użytkowników oraz w miarę możliwości udostępnia zgodnie z prawem ochrony danych rozwiązania równoważne.

17. Projektowanie prywatności
Firma zarządza zmianą mającą wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania.
W tym celu zasady prowadzenia projektów i inwestycji przez Firmę odwołują się do zasad bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę danych osobowych, uwzględnienia i zaprojektowania bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub inwestycji.

18. Postanowienia końcowe
Stosownie do potrzeb możemy zmieniać i uzupełniać Politykę Prywatności. O wszelkich zmianach lub uzupełnieniach poinformujemy Cię poprzez zamieszczenie odpowiednich informacji na naszej stronie www.turystykakika.pl a w przypadku istotnych zmian możemy wysłać Ci także odrębne powiadomienia na wskazany przez Ciebie adres e-mail.
Polityka Prywatności nie ogranicza żadnych uprawnień przysługujących Ci zgodnie z Regulaminem Ośrodka „Kika”oraz przepisami prawa.