Ruda Śląska, dnia 11 października 2021 roku

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

obowiązująca w jednoosobowej działalności gospodarczej

prowadzonej przez Arletę Żymła pod firmą:

„RUN & SKI TRAVEL ARLETA ŻYMŁA”

z siedzibą w Rudzie Śląskiej (41-707) przy ul. Jacka 26

NIP: 6412453085, REGON: 241017689

(dalej jako: „Podmiot” lub „Run & Ski Travel”)

I WPROWADZENIE

Polityka Bezpieczeństwa Danych Osobowych, zwana dalej Polityką, została sporządzona w związku z wymaganiami 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 – dalej Rozporządzenie UE) oraz ustawy o ochronie danych osobowych.

Niniejszy dokument stanowi zbiór spójnych, precyzyjnych reguł i procedur, według których Run & Ski Travel buduje, zarządza oraz udostępnia zasoby i systemy informacyjne i informatyczne. Ustanawia przewidziane do wykonania działania oraz sposób ustanowienia zasad i reguł postępowania koniecznych do zapewnienia właściwej ochrony przetwarzanych danych osobowych. Polityka ustanawia zasady bezpieczeństwa przetwarzania danych osobowych, które powinny być przestrzegane i stosowane przez wszystkie osoby przetwarzające dane osobowe w Podmiocie wraz z powołaniem na właściwe podstawy prawne. Polityka reguluje zasady organizacji pracy przy zbiorach danych osobowych przetwarzanych w systemie informatycznym oraz metodami tradycyjnymi. Opisano w niej również zagrożenia bezpieczeństwa przetwarzanych danych osobowych oraz sposoby reakcji na przypadki naruszeń bezpieczeństwa.

Niniejszy dokument pełni również funkcję informacyjną i edukacyjną, poprzez zaprezentowanie obowiązków i odpowiedzialności osób związanych z przetwarzaniem danych osobowych.

Run & Ski Travel stosuje adekwatne do sytuacji środki, aby zapewnić bezpieczeństwo informacji.

Uzupełnieniem i dopełnieniem niniejszej Polityki jest Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych (Załącznik nr 1), ustanawiająca sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych.

II PODSTAWA PRAWNA

Zasady przetwarzania danych osobowych w szczególności regulują:

- ✓ 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
- ✓ Ustawa o ochronie danych osobowych z dnia 10 maja 2018 roku

III SŁOWNICZEK

ADO – Administrator Danych Osobowych, będący organem, jednostką organizacyjną, podmiotem lub osobą fizyczną, decydujący o celach i środkach przetwarzania danych osobowych, w rozumieniu niniejszej Polityki jest Arleta Żymła prowadząca jednoosobową działalność gospodarczą pod firmą: „Run & Ski Travel Arleta Żymła", adres głównego miejsca prowadzenia działalności gospodarczej: ul. Jacka 26, 41-717 Ruda Śląska, NIP: 6412453085 oraz REGON: 241017689.

Dane osobowe - wszelkie informacje dotyczące 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.

Dane wrażliwe (szczególna kategoria danych) - dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej oraz dane dotyczące wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa.

PUODO – Prezes Urzędu Ochrony Danych Osobowych, będący organem powołanym do spraw z zakresu ochrony danych osobowych.

Polityka – niniejszy dokument Polityki Bezpieczeństwa Danych Osobowych.

Przetwarzanie danych – 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.

System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Upoważniony – osoba posiadająca formalne upoważnienie wydane przez Administratora Danych Osobowych lub przez osobę wyznaczoną, uprawniona do przetwarzania danych osobowych.

Usuwanie danych – zniszczenie danych osobowych lub ich modyfikacja, która uniemożliwia ustalenie tożsamości osoby, której dane dotyczą.

Zabezpieczenie danych w systemie informatycznym – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

Zbiór danych – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

Zgoda osoby, której dane dotyczą – oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

IV PRZETWARZANIE DANYCH OSOBOWYCH

Dane osobowe

Za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Przy rozstrzyganiu czy określona informacja lub informacje stanowią dane osobowe, Run & Ski Travel dokonuje zindywidualizowanej oceny, przy uwzględnieniu konkretnych okoliczności oraz rodzaju środków czy metod potrzebnych w określonej sytuacji do identyfikacji osoby.

Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Danymi osobowymi będą zarówno takie dane, które pozwalają na określenie tożsamości konkretnej osoby, jak i takie, które nie pozwalają na jej natychmiastową identyfikację, ale są, przy pewnym nakładzie kosztów, czasu i działań, wystarczające do jej ustalenia.

Przetwarzanie danych osobowych

Przy wykonywaniu tej działalności gospodarczej Run & Ski Travel pozyskuje i przetwarza dane osobowe. Dane te mieszczą się w następujących kategoriach (kategorie danych osobowych):

1. Zbiór danych osobowych klientów sklepu internetowego,

2. Zbiór danych osobowych osób fizycznych wykonujących usługi i dostarczających towary, na podstawie umów cywilnoprawnych (w tym specjaliści tacy jak osoby świadczące usługi księgowe, informatyczne, prawnicze – w zależności od formy działalności),
3. Zbiór danych osobowych osób zatrudnionych w strukturze osób prawnych i jednostek organizacyjnych niebędących osobami prawnymi, którym ustawa przyznaje zdolność prawną, wykonujących usługi i dostarczających towary, na podstawie umów cywilnoprawnych (w tym specjaliści tacy jak osoby świadczące usługi księgowe, informatyczne, prawnicze – w zależności od formy działalności).

Mając na uwadze przepisy w zakresie ochrony danych osobowych Run & Ski Travel przetwarza dane osobowe tylko wtedy, gdy:

1. osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
2. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
3. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
4. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
5. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
6. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą, jest dzieckiem.

Run & Ski Travel co do zasady nie przetwarza danych wrażliwych (szczególnej kategorii danych), jeśli jednak doszłoby do takiego przetwarzania, Run & Ski Travel będzie przetwarzało je tylko w sytuacji, gdy:

1. osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu;
2. przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej;
3. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
4. przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;

5. przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
6. przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;
7. przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego;
8. przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;
9. przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

Obowiązki informacyjne o przetwarzaniu danych

W przypadku zbierania danych od osoby, której te dane dotyczą Run & Ski Travel jako Administrator Danych Osobowych podaje jej wszystkie następujące informacje:

1. swoją tożsamość i dane kontaktowe oraz gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
2. cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania;
3. jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) Rozporządzenia UE – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;
4. informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
5. gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony;
6. okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

7. informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
8. jeżeli przetwarzanie odbywa się na podstawie zgody – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
9. informacje o prawie wniesienia skargi do organu nadzorczego;
10. informacje czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
11. informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 Rozporządzenia UE, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Podanych wyżej zasad nie stosuje się, jeżeli przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania lub jeżeli osoba, której dane dotyczą, posiada już te informacje.

W przypadku zbierania danych nie od osoby, której te dane dotyczą Run & Ski Travel jako Administrator Danych Osobowych jest zobowiązany poinformować tę osobę bezpośrednio po utrwaleniu danych dodatkowo o:

1. źródle pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych;
2. kategoriach odnośnych danych osobowych.

Podanych wyżej zasad nie stosuje się, jeżeli:

1. przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą,
2. poinformowanie wymaga niewspółmiernie dużego wysiłku – w szczególności, gdy dane przetwarzane są w celach archiwizacyjnych, statystycznych, badań naukowych,
3. przekazanie informacji okazuje się niemożliwe,
4. utrwalenie lub ujawnienie danych jest wyraźnie nakazane prawem UE lub prawa krajowego,
5. dotyczy to tajemnicy zawodowej wynikającej z prawa UE lub prawa krajowego.

Zasady przetwarzania danych

Run & Ski Travel realizuje obowiązki poprzez dołożenie szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, zapewniając, aby dane te były:

1. przetwarzane zgodnie z prawem,

(Zgodne z wszelkimi normami prawa, zarówno tymi już istniejącymi w momencie wejścia w życie Rozporządzenia UE, jak i tymi, które dopiero później zostały wprowadzone do porządku prawnego. Zgodność z prawem dotyczy przestrzegania zarówno przepisów prawa materialnego, jak i przepisów dotyczących postępowania).

2. zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,

3. merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,

(Informacje wynikające z danych przetwarzanych przez administratora są zgodne z prawdą, kompletne oraz odpowiadają aktualnemu stanowi rzeczy. Administrator Danych Osobowych przetwarza dane tylko w takim zakresie, w jakim jest to niezbędne do wypełnienia celu, w jakim dane są przez niego przetwarzane).

4. przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

5. Administrator Danych Osobowych stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Dodatkowo Podmiot zapewnia bezpieczeństwo informacji poprzez:

1. poufność informacji
   (informacje nie są udostępniane lub wyjawiane osobom nieupoważnionym, osoby nieuprawnione nie mają dostępu do danych),
2. integralność informacji
   (informacje są kompletne i niezmieniane w sposób nieuprawniony),
3. rozliczalność działań
   (wszystkie istotne czynności wykonane przy przetwarzaniu danych zostały zarejestrowane i jest możliwe zidentyfikowanie osoby, która daną czynność wykonała),
4. niezawodność działań
   (wykonywane czynności prowadzi do zamierzonych skutków).

Powierzenie przetwarzania danych

W przypadku konieczności przetwarzania danych przez odrębne podmioty świadczące usługi dla Administratora Danych Osobowych może on powierzyć ich przetwarzanie. Powierzenie przetwarzania odbywa się na podstawie umowy lub innego instrumentu prawnego, które

podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

Wzór umowy powierzenia danych stanowi załącznik do niniejszej Polityki (zał. nr 6).

Run & Ski Travel prowadzi dokument Ewidencji podmiotów, którym Podmiot powierza dane osobowe.

(Ewidencja podmiotów, którym Podmiot powierza dane osobowe stanowi załącznik do niniejszej Polityki (załącznik nr 4).

Udostępnianie danych

Run & Ski Travel może udostępnić dane osobowe poprzez działania umożliwiające innym niż administrator podmiotom, zapoznanie się z nimi, zachowując wymogi nałożone przez prawo. Przy czym:

1. Nie jest istotne czy udostępnianie danych ma charakter odpłatny czy nie, aby czynność była uznana za udostępnianie.
2. Nie jest istotne, czy udostępnianie następuje w formie przekazu ustnego, pisemnego, za pomocą powszechnych środków przekazu lub poprzez sieć komputerową itd., aby czynność była uznana za udostępnianie.
3. Udostępnianie danych osobowych osobom lub podmiotom uprawnionym do ich otrzymania odbywa się na mocy przepisów prawa.
4. Udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

Na skutek udostępnienia danych osobowych dochodzi do faktycznego przekazania danych osobowych, w wyniku którego nowy dysponent tych danych staje się ich administratorem, a co za tym idzie będzie decydował o celach i środkach przetwarzania danych, oraz ponosił odpowiedzialność w zakresie przewidzianym dla administratora. Warunki udostępnienia, w tym sposób przekazania klauzuli informacyjnej, zostaną każdorazowo uzgodnione w umowie pomiędzy Run & Ski Travel a podmiotem, któremu dane zostaną udostępnione lub współudostępnione.

Rejestrowanie czynności przetwarzania

Run & Ski Travel prowadzi rejestr czynności przetwarzania danych osobowych, za które odpowiada.

W rejestrze tym zamieszcza wszystkie następujące informacje:

1. imię i nazwisko lub nazwę oraz dane kontaktowe administratora, a także gdy ma to zastosowanie wszelkich współadministratorów oraz inspektora ochrony danych;
2. cele przetwarzania;
3. opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
4. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
5. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi Rozporządzenia UE, dokumentacja odpowiednich zabezpieczeń;
6. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
7. jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.

Rejestr czynności przetwarzania danych osobowych stanowi załącznik nr 7 do niniejszej Polityki.

V UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Do przetwarzania danych osobowych uprawnione są wyłącznie osoby Upoważnione do przetwarzania danych osobowych.
2. Celem niniejszej procedury jest minimalizacja ryzyka nieuprawnionego dostępu do danych osobowych i utraty ich poufności przez osoby nieupoważnione.
3. Administrator Danych Osobowych jest uprawniony do przyznawania upoważnień w przedmiocie przetwarzania danych osobowych, w drodze pisemnego Upoważnienia do przetwarzania danych osobowych (wzór upoważnienia stanowi załącznik nr 3).
4. Administrator Danych Osobowych może wyznaczyć osoby uprawnione do przyznawania upoważnień w przedmiocie przetwarzania danych osobowych, w drodze pisemnego uprawnienia.
5. Upoważnienie do przetwarzania danych osobowych następuje wyłącznie na podstawie indywidualnego upoważnienia nadanego zgodnie z przepisami ustawy o ochronie danych osobowych.
6. Nadanie upoważnienia do przetwarzania danych osobowych musi nastąpić przed rozpoczęciem przetwarzania danych przez osobę upoważnioną.
7. Administrator Danych Osobowych lub osoba przez niego upoważniona prowadzi dokument Ewidencji osób upoważnionych do przetwarzania danych osobowych (załącznik nr 2).
8. W przypadku konieczności nadania bądź zmiany uprawnień (np. z powodu zatrudnienia osoby lub zmiany stanowiska pracy), Administrator Danych Osobowych lub osoba przez niego upoważniona zobowiązany jest do sprawdzenia, czy dana osoba będzie przetwarzała dane osobowe w zakresie i celu określonym w Polityce i instrukcji zarządzania systemem informatycznym.

9. Nadanie upoważnienia do przetwarzania danych osobowych wymaga zaznajomienia się z przepisami dotyczącymi ochrony danych osobowych, w zakresie niezbędnym do czynności wykonywanych w ramach udzielonego upoważnienia.
10. Administrator Danych Osobowych jest odpowiedzialny za organizację i przeprowadzenie szkoleń lub zaznajomienie w innej formie osób upoważnionych z przepisami dotyczącymi ochrony danych osobowych.

VI OBOWIĄZKI PODMIOTOWE W OBSZARZE OCHRONY DANYCH OSOBOWYCH

Obowiązki Administratora Danych Osobowych

1. podział zadań i obowiązków związanych z organizacją ochrony danych osobowych,
2. podejmowanie odpowiednich i niezbędnych działań mających na celu zapewnienie prawidłowej ochrony danych osobowych, w szczególności poprzez sporządzanie i wdrażanie właściwych warunków organizacyjnych i technicznych,
3. wprowadzenie do stosowania procedur zapewniających prawidłowe przetwarzanie danych osobowych,
4. w przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je PUODO, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych,
5. dokonanie oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych w sytuacjach, gdy wymagają tego przepisu prawa,
6. egzekwowanie rozwoju środków bezpieczeństwa przetwarzania danych osobowych,
7. poddawanie przeglądom skuteczność Polityki bezpieczeństwa przetwarzania danych osobowych,
8. zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez: organizację i nadzorowanie przestrzegania zasad ochrony danych osobowych zarówno w systemach informatycznych, jak również w zbiorach danych osobowych prowadzonych w formie papierowej i elektronicznej,
9. prowadzenie dokumentacji opisującej zastosowaną politykę bezpieczeństwa przetwarzania danych osobowych (niniejsza Polityka oraz wynikające z niej instrukcje i procedury),
10. wdrożenie zapoznania z przepisami dotyczącymi ochrony danych osobowych oraz zagrożeniami związanymi z przetwarzaniem danych przez osoby będące członkami Podmiotu,
11. zapewnienie kontroli nad tym, jakie dane osobowe, przez kogo i kiedy zostały wprowadzone do zbioru,
12. nadawanie i uchylanie uprawnień do przetwarzania danych osobowych w Podmiocie,
13. prowadzenie rejestru osób Upoważnionych do przetwarzania danych, zawierającego imię i nazwisko Upoważnionego, datę nadania i ustania, zakres Upoważnienia do przetwarzania

danych osobowych, identyfikator w przypadku, gdy Upoważniony został zarejestrowany w systemie informatycznym, służącym do przetwarzania danych osobowych,

14. zapewnienie zapoznania osób Upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
15. analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia ochrony danych osobowych i przygotowanie zaleceń i rekomendacji dotyczących eliminacji ryzyka ich ponownego wystąpienia,
16. prowadzenie zgodnych z Instrukcją działań w przypadku stwierdzenia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych,
17. zapewnienie podstaw prawnych do przetwarzania danych osobowych od chwili zebrania danych osobowych do chwili ich usunięcia,
18. dbałość o prawidłowe przetwarzanie danych osobowych, w szczególności poprzez zapewnienie aktualności, adekwatności oraz merytorycznej poprawności danych osobowych przetwarzanych w określonym przez nich celu.

Obowiązki Upoważnionych

1. znajomość Polityki oraz przepisów powszechnie obowiązującego prawa w obszarze ochrony danych osobowych, przetwarzanych przez Podmiot,
2. znajomość, zrozumienie i stosowanie w możliwie największym zakresie wszelkich dostępnych środków ochrony danych osobowych oraz uniemożliwienie osobom nieuprawnionym dostępu do swojej stacji roboczej,
3. przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa oraz przyjętymi regulacjami, w granicach przyznanego upoważnienia,
4. postępowanie zgodnie z ustalonymi regulacjami wewnętrznymi dotyczącymi przetwarzania danych osobowych,
5. zachowanie w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia, również po ustaniu zatrudnienia,
6. ochrona danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem,
7. informowanie o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe do przełożonego, który ma obowiązek poinformować Administratora Bezpieczeństwa Informacji.

VII OCENA RYZYKA I PRZEGLĄDY

Jeżeli dany rodzaj przetwarzania danych osobowych – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Run & Ski Travel przed rozpoczęciem przetwarzania dokona oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, zgodnie z art. 35 RODO.

VIII ZAGROŻENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH ORAZ INCYDENTY

Na bezpieczeństwo procesu przetwarzania danych osobowych składają się rozliczalność, poufność i integralność przetwarzanych danych. Rozliczalność oznacza możliwość przypisania działań osoby jednoznacznie i wyłącznie tej osobie. Poufność wyraża się zapewnieniem, że przetwarzane dane osobowe nie są udostępniane nieupoważnionym podmiotom. Integralność oznacza zapewnienie niemożliwości zmiany lub nieautoryzowanego zniszczenia danych osobowych.

W przypadku stwierdzenia naruszenia ochrony danych osobowych lub ich zagrożenia, każdy podmiot upoważniony do przetwarzania danych osobowych w imieniu Run & Ski Travel jest zobowiązany poinformować o tym fakcie Administratora Danych Osobowych i/lub właściwą osobę przez niego upoważnioną.

Instrukcja postępowania w przypadku zagrożenia bezpieczeństwa danych osobowych

Zagrożeniem bezpieczeństwa informacji jest sytuacja, w której występuje zagrożenie zaistnienia incydentu. Przykładowy katalog zagrożeń:

1. nieprzestrzeganie Polityki przez osoby przetwarzające dane, np. niezamykanie pomieszczeń, szaf, biurek, brak stosowania zasad ochrony haseł,
2. niewłaściwe zabezpieczenie fizyczne dokumentów, urządzeń lub pomieszczeń,
3. niewłaściwe zabezpieczenie oprogramowania lub sprzętu IT przed wyciekiem, kradzieżą lub utratą danych osobowych.

Postępowanie Administratora Danych Osobowych lub osoby przez niego upoważnionej w przypadku stwierdzenia wystąpienia zagrożenia:

1. ustalenie zakresu i przyczyn zagrożenia oraz jego ewentualnych skutków,
2. w miarę możliwości przywrócenie stanu zgodnego z zasadami ochrony danych osobowych,
3. w razie konieczności zainicjowanie działań dyscyplinarnych,
4. zarekomendowanie działań zapobiegawczych w kierunku wyeliminowania podobnych zagrożeń w przyszłości,
5. udokumentowanie prowadzonego postępowania w Rejestrze naruszeń bezpieczeństwa (załącznik nr 5).

Instrukcja postępowania w przypadku incydentów bezpieczeństwa danych osobowych

Incydentem jest sytuacja naruszenia bezpieczeństwa informacji ze względu na dostępność, integralność i poufność. Incydenty powinny być wykrywane, rejestrowane i monitorowane w celu zapobieżenia ich ponownemu wystąpieniu. Przykładowy katalog incydentów:

1. losowe zdarzenie wewnętrzne, np. awaria komputera, serwera, twardego dysku, błąd użytkownika, informatyka, zgubienie danych,
2. losowe zdarzenie zewnętrzne, np. klęski żywiołowe, zalanie, awaria zasilania, pożar,
3. incydent umyślny, np. wyciek informacji, ujawnienie danych nieupoważnionym osobom, świadome zniszczenie danych, działanie wirusów komputerowych, włamanie do pomieszczeń lub systemu informatycznego (wewnętrzne i zewnętrzne).

Postępowanie Administratora Danych Osobowych lub właściwej osoby przez niego upoważnionej w przypadku stwierdzenia wystąpienia incydentu:

1. ustalenie czasu zdarzenia będącego incydentem,
2. ustalenie zakresu incydentu,
3. określenie przyczyn, skutków oraz szacowanych zaistniałych szkód,
4. zabezpieczenie dowodów,
5. ustalenie osób odpowiedzialnych za naruszenie,
6. usunięcie skutków incydentu,
7. ograniczenie szkód wywołanych incydentem,
8. zainicjowanie działań dyscyplinarnych,
9. zarekomendowanie działań zapobiegawczych w kierunku wyeliminowania podobnych zagrożeń w przyszłości,
10. udokumentowanie prowadzonego postępowania w Rejestrze naruszeń bezpieczeństwa (załącznik nr 5).

Postępowanie Upoważnionego w przypadku stwierdzenia wystąpienia zagrożenia do czasu przybycia Administratora Danych Osobowych lub upoważnionej przez niego osoby:

1. powstrzymanie się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów,
2. zabezpieczenie elementów systemu informatycznego lub kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osób nieupoważnionych,
3. podjęcie, stosownie do zaistniałej sytuacji, wszelkich niezbędnych działań celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.

IX WYKAZY

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane dane osobowe.

Lp.	Adres	Pomieszczenia	Zastosowane zabezpieczenia
1.	ul. Jacka 26 41-707 Ruda Śląska		- budynek zamykany z domofonem i monitoringiem; - w lokalu zabezpieczenie drzwiami antywłamaniowymi; - dokumenty zabezpieczone w szafkach;
2.	dane elektroniczne na urządzeniu przenośnym	Laptop marki ___, model _____Nr seryjny: _____	Program antywirusowy, dostęp zabezpieczony hasłem;
3.			

X POSTANOWIENIA KOŃCOWE

1. Polityka bezpieczeństwa jest dokumentem obowiązującym w Podmiocie w zakresie wdrażania, przestrzegania i weryfikacji zasad ochrony danych osobowych.
2. Polityka bezpieczeństwa jest dokumentem obowiązującym wszystkie osoby dopuszczone do przetwarzania danych osobowych w ramach działalności Run & Ski Travel.
3. Każda osoba dopuszczona do przetwarzania danych osobowych w ramach działalności Podmiotu ma obowiązek zapoznania się z niniejszą Polityką bezpieczeństwa.
4. Naruszenie zasad wynikających z Polityki bezpieczeństwa może stanowić podstawę wszczęcia postępowania dyscyplinarnego przeciwko sprawcy naruszenia lub rozwiązania umowy zlecenia ze skutkiem natychmiastowym bez zachowania okresu wypowiedzenia.
5. Wszczęcie lub przeprowadzenie postępowania dyscyplinarnego przeciwko osobie naruszającej zasady wynikające z Polityki bezpieczeństwa nie wyklucza możliwości wszczęcia postępowania karnego oraz dochodzenia roszczeń z powództwa cywilnego.
6. Polityka bezpieczeństwa wraz z załącznikami wchodzi w życie z dniem jej podpisania przez Arletę Żymła prowadzącą jednoosobową działalność gospodarczą Run & Ski Travel.
7. W przedmiocie spraw nieuregulowanych Polityką bezpieczeństwa, zastosowanie znajdują przepisy ustawy o ochronie danych osobowych.
8. Załączniki do niniejszej Polityki stanowią jej część pod warunkiem uzupełnienia.

Lista załączników:

- Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych (zał. nr 1),
- Ewidencja osób upoważnionych do przetwarzania danych osobowych (zał. nr 2),
- Upoważnienie do przetwarzania danych osobowych – wzór (zał. nr 3),
- Ewidencja podmiotów, którym Podmiot powierza dane osobowe (zał. nr 4),
- Rejestr naruszeń bezpieczeństwa (zał. nr 5),
- Wzór umowy powierzenia danych osobowych (zał. 6),
- Rejestr czynności przetwarzania danych osobowych (zał. 7),

Podpis Administratora Danych Osobowych	Data