

POLITYKA OCHRONY DANYCH OSOBOWYCH

1. Niniejszy dokument zatytułowany „Polityka ochrony danych osobowych” (dalej zwany „Polityką”) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych u przedsiębiorcy Andrzeja Szczepanka prowadzącego działalność gospodarczą pod nazwą: Hugart Hotels Andrzej Szczepanek (dalej zwanego „OW Kolejarz”), NIP: 642-181-44-01 z siedzibą: ul. Chełmońskiego 1, 44-200 Rybnik, przy czym działalność w zakresie usług noclegowych, restauracyjnych, rekreacji i odnowy biologicznej (SPA, masaże, itp.) prowadzona jest pod adresem: OW Kolejarz, ulica Stroma 2, 43-450 Ustroń. Jeśli w Polityce mowa jest o OW Kolejarz zawsze oznacza to w zakresie miejsca położenia obiekt usytuowany pod adresem: ulica Stroma 2, 43-450 Ustroń.
2. Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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.Urz. UE L 119, s. 1).
3. Polityka zawiera:
 - a) opis zasad ochrony danych obowiązujących w OW Kolejarz,
 - b) odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach).
4. Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest Andrzej Szczepanek.
5. Za nadzór i monitorowanie przestrzegania Polityki oraz zgodność działań OW Kolejarz z przepisami prawa dotyczącymi ochrony danych osobowych odpowiadają:
 - a) Inspektor Ochrony Danych powołany na podstawie pełnomocnictwa udzielonego przez Andrzeja Szczepanka,
 - b) komórka audytu wewnętrznego powołana na podstawie pisemnej decyzji Andrzeja Szczepanka.
6. Za stosowanie Polityki odpowiedzialni są (w następującej kolejności ważności):
 - a) Andrzej Szczepanek,
 - b) osoby sprawujące funkcje kierownicze w poszczególnych komórkach organizacyjnych OW Kolejarz przetwarzających dane osobowe,
 - c) pracownicy poszczególnych komórek organizacyjnych przetwarzający dane osobowe,
 - d) wszyscy pozostali pracownicy i współpracownicy OW Kolejarz.
7. OW Kolejarz zapewnia zgodność postępowania kontrahentów OW Kolejarz z Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez OW Kolejarz.

8. Skróty i definicje.

- a) **Polityka** oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu niniejszego dokumentu,
- b) **RODO** oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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.Urz. UE L 119, s. 1),
- c) **Dane lub Dane Osobowe** oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu Polityki,
- d) **Dane wrażliwe** oznaczają dane specjalne i dane karne,
- e) **Dane specjalne** 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,
- f) **Dane karne** oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa,
- g) **Dane dzieci** oznaczają dane osób poniżej 16 roku życia,
- h) **Osoba** oznacza osobę fizyczną, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu Polityki,
- i) **Podmiot przetwarzający** oznacza organizację lub osobę, której OW Kolejarz powierzył przetwarzanie danych osobowych (np. usługodawca IT, zewnętrzna księgowość),
- j) **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,
- k) **Eksport danych** oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej,
- l) **IOD lub Inspektor** oznacza Inspektora Ochrony Danych Osobowych **RCPD lub Rejestr** oznacza Rejestr Czynności Przetwarzania Danych Osobowych,
- m) OW Kolejarz oznacza przedsiębiorcę Andrzeja Szczepanka prowadzącego działalność gospodarczą pod nazwą: Hugart Hotels Andrzej Szczepanek, NIP: 642-181-44-01.

9. Filary ochrony Danych Osobowych w OW Kolejarz.

- a) legalność – OW Kolejarz dba o ochronę prywatności i przetwarza Dane zgodnie z prawem,
- b) bezpieczeństwo – OW Kolejarz zapewnia odpowiedni poziom bezpieczeństwa Danych, podejmując stale działania w tym zakresie,
- c) prawa jednostki – OW Kolejarz umożliwia Osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje,
- d) rozliczalność – OW Kolejarz dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność postępowania z Polityką i RODO.

10. Zasady ochrony danych.

OW Kolejarz 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 dotyczą (transparentność),
- d) wyłącznie w konkretnych celach i nie „na zapas” (minimalizacja),
- e) nie więcej niż potrzeba (adekwatność),
- f) z dbałością o prawidłowość Danych (prawidłowość),
- g) nie dłużej niż potrzeba (czasowość),
- h) zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

11. System ochrony Danych.

System ochrony Danych Osobowych w OW Kolejarz składa się z następujących elementów:

- a) **Inwentaryzacja Danych, tj.** OW Kolejarz dokonuje identyfikacji zasobów Danych Osobowych w OW Kolejarz, klas Danych, zależności między zasobami Danych, identyfikacji sposobów wykorzystania Danych (inwentaryzacja), w tym:
 - (i) przypadków przetwarzania Danych wrażliwych,
 - (ii) przypadków przetwarzania Danych Osób, których OW Kolejarz nie identyfikuje (**dane niezidentyfikowane/UFO**),
 - (iii) przypadków przetwarzania Danych Dzieci,
 - (iv) profilowania,
 - (v) współadministrowania Danymi.
- b) **Rejestr.** OW Kolejarz opracowuje, prowadzi i utrzymuje Rejestr Czynności Danych Osobowych w OW Kolejarz (dalej zwanym „Rejestrem”). Rejestr jest narzędziem rozliczania zgodności z ochroną Danych w OW Kolejarz.
- c) **Podstawy prawne.** OW Kolejarz zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania Danych i rejestruje je w Rejestrze, w tym:
 - (i) utrzymuje system zarządzania zgodami na przetwarzanie Danych i komunikację na odległość,
 - (ii) inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy OW Kolejarz przetwarza Dane na podstawie prawnie uzasadnionego interesu OW Kolejarz.
- d) **Obsługa praw jednostki.** OW Kolejarz spełnia obowiązki informacyjne względem Osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
 - (i) **Obowiązki informacyjne.** OW Kolejarz przekazuje osobom prawem wymagane informacje przy zbieraniu Danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków.
 - (ii) **Możliwość wykonania żądań Osób, których Dane dotyczą.** OW Kolejarz weryfikuje i zapewnia możliwość efektywnego

wykonania każdego typu żądania przez siebie i swoich przetwarzających.

- (iii) **Obsługa żądań.** OW Kolejarz zapewnia odpowiednie nakłady i procedury aby żądania Osób były realizowane w terminach i w sposób wymagany RODO i dokumentowane.
- (iv) **Zawiadamianie o naruszeniach.** OW Kolejarz stosuje procedury pozwalające na ustalenie konieczności zawiadomienia Osób dotkniętych zidentyfikowanym naruszeniem ochrony Danych.
- (v) **Minimalizacja.** OW Kolejarz posiada zasady i metody zarządzania minimalizacją (*privacy by default*), a w tym:
 - zasady zarządzania adekwatnością Danych;
 - zasady reglamentacji i zarządzania dostępem do Danych;
 - zasady zarządzania okresem przechowywania Danych i weryfikacji dalszej przydatności;
- (vi) **Bezpieczeństwo.** OW Kolejarz zapewnia odpowiedni poziom bezpieczeństwa Danych, w tym:
 - przeprowadza analizy ryzyka dla czynności przetwarzania Danych lub ich kategorii,
 - przeprowadza oceny skutków dla ochrony Danych tam, gdzie ryzyko naruszenia praw i wolności Osób jest wysokie,
 - dostosowuje środki ochrony Danych do ustalonego ryzyka,
 - posiada system zarządzania bezpieczeństwem informacji,
 - stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony Danych Urzędowi Ochrony Danych – zarządza incydentami.
- (vii) **Przetwarzający.** OW Kolejarz posiada zasady doboru przetwarzających Dane na rzecz OW Kolejarz, wymogów co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia.
- (viii) **Eksport danych.** OW Kolejarz posiada zasady weryfikacji, czy OW Kolejarz nie przekazuje Danych do państw trzecich (czyli poza UE, Norwegię, Lichtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków takiego przekazywania, jeśli ma ono miejsce.
- (ix) **Privacy by design.** OW Kolejarz zarządza zmianami mającymi wpływ na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji w OW Kolejarz uwzględniają konieczność oceny wpływu zmiany na ochronę Danych, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa Danych i minimalizacji) już w

fazie projektowania zmiany, inwestycji czy na początku nowego projektu.

- (x) **Przetwarzanie transgraniczne.** OW Kolejarz posiada zasady weryfikacji, kiedy zachodzą przypadki przetwarzania transgranicznego oraz zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO.

12. Inwentaryacja Danych wrażliwych.

OW Kolejarz identyfikuje przypadki, w których przetwarza lub może przetwarzać Dane wrażliwe (Dane specjalne i Dane karne) oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania Danych wrażliwych. W przypadku zidentyfikowania przypadków przetwarzania Danych wrażliwych, OW Kolejarz postępuje zgodnie z prawem i zgodnie z treścią Polityki.

13. Inwentaryacja Danych niezidentyfikowanych.

OW Kolejarz identyfikuje przypadki, w których przetwarza lub może przetwarzać Dane niezidentyfikowane i utrzymuje mechanizmy ułatwiające realizację praw Osób, których dotyczą Dane niezidentyfikowane.

14. Profilowanie.

OW Kolejarz identyfikuje przypadki, w których dokonuje profilowania przetwarzanych Danych i utrzymuje mechanizmy zapewniające zgodność tego procesu z prawem. W przypadku zidentyfikowania przypadków profilowania i zautomatyzowanego podejmowania decyzji, OW Kolejarz postępuje zgodnie z prawem i zgodnie z treścią Polityki.

15. Współadministrowanie.

OW Kolejarz identyfikuje przypadki współadministrowania Danymi i postępuje w tym zakresie zgodnie z prawem i treścią Polityki.

16. Rejestr Czynności Przetwarzania Danych.

1. Rejestr stanowi formę dokumentowania czynności przetwarzania Danych, pełni rolę mapy przetwarzania Danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony Danych osobowych, czyli zasady rozliczalności.
2. OW Kolejarz prowadzi Rejestr, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje Dane.
3. Rejestr jest jednym z podstawowych narzędzi umożliwiających OW Kolejarz rozliczanie większości obowiązków ochrony Danych.
4. W Rejestrze, dla każdej czynności przetwarzania danych, którą OW Kolejarz uznał za odrębną dla potrzeb Rejestru, OW Kolejarz odnotowuje co najmniej:

- (i) nazwę czynności,

- (ii) cel przetwarzania,
 - (iii) opis kategorii Osób,
 - (iv) opis kategorii Danych,
 - (v) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu OW Kolejarz, jeśli podstawą jest uzasadniony interes OW Kolejarz,
 - (vi) sposób zbierania Danych,
 - (vii) opis kategorii odbiorców Danych (w tym przetwarzających),
 - (viii) informację o przekazaniu poza EU/EOG,
 - (ix) ogólny opis technicznych i organizacyjnych środków ochrony Danych.
5. Wzór Rejestru stanowi **Załącznik nr 1 do Polityki – „Wzór Rejestru Czynności Przetwarzania Danych”**. Wzór Rejestru zawiera także kolumny nieobowiązkowe. W kolumnach nieobowiązkowych OW Kolejarz rejestruje informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść Rejestru ułatwia zarządzanie zgodnością ochrony Danych i rozliczenie się z niej.

17. Podstawy przetwarzania.

1. OW Kolejarz dokumentuje w Rejestrze podstawy prawne przetwarzania Danych dla poszczególnych czynności przetwarzania.
2. Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony interes OW Kolejarz) OW Kolejarz dookreśla podstawę w czytelny sposób, gdy jest to potrzebne, np. dla zgody wskazując na jej zakres, gdy podstawą jest prawo – wskazując na konkretny przepis i inne dokumenty, np. umowę, porozumienie administracyjne, żywotne interesy – wskazując na kategorie zdarzeń, w których się zmaterializują, uzasadniony cel – wskazując na konkretny cel, np. marketing własny, dochodzenie roszczeń.
3. OW Kolejarz wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody Osoby na przetwarzanie jej konkretnych Danych w konkretnym celu, zgody na komunikację na odległość (email, telefon, sms, in.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).
4. Kierownik komórki organizacyjnej OW Kolejarz ma obowiązek znać podstawy prawne, na jakich komórka przez niego kierowana dokonuje konkretnych czynności przetwarzania Danych Osobowych. Jeżeli podstawą jest uzasadniony interes OW Kolejarz, kierownik komórki ma obowiązek znać konkretny realizowany przetwarzaniem interes OW Kolejarz.

18. Sposób obsługi praw jednostki i obowiązków informacyjnych.

1. OW Kolejarz dba o czytelność i styl przekazywanych informacji i komunikacji z Osobami, których Dane przetwarza.
2. OW Kolejarz ułatwia Osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczenie na stronie internetowej OW Kolejarz informacji lub odwołań (linków) do informacji o prawach Osób, sposobie skorzystania z nich

w OW Kolejarz, w tym wymaganiach dotyczących identyfikacji, metodach kontaktu z OW Kolejarz w tym celu, ewentualnym cenniku żądań „dodatkowych” itp.

3. OW Kolejarz dba o dotrzymanie prawnych terminów realizacji obowiązków względem Osób.
4. OW Kolejarz wprowadza adekwatne metody identyfikacji i uwierzytelniania Osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.
5. W celu realizacji praw jednostki OW Kolejarz zapewnia procedury i mechanizmy pozwalające zidentyfikować Dane konkretnych Osób przetwarzane przez OW Kolejarz, zintegrować te Dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany.
6. OW Kolejarz dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań Osób.

19. Obowiązki informacyjne.

1. OW Kolejarz określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.
2. OW Kolejarz informuje Osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej Osoby.
3. OW Kolejarz informuje Osobę o przetwarzaniu jej Danych, przy pozyskiwaniu Danych od tej osoby.
4. OW Kolejarz informuje Osobę o przetwarzaniu jej Danych, przy pozyskiwaniu Danych o tej Osobie niebezpośrednio od niej.
5. OW Kolejarz określa sposób informowania Osób o przetwarzaniu Danych niezidentyfikowanych, tam gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym).
6. OW Kolejarz informuje Osobę o planowanej zmianie celu przetwarzania Danych.
7. OW Kolejarz informuje Osobę przed uchyleniem ograniczenia przetwarzania.
8. OW Kolejarz informuje odbiorców Danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania Danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).
9. OW Kolejarz informuje Osobę o prawie sprzeciwu względem przetwarzania Danych najpóźniej przy pierwszym kontakcie z tą Osobą.
10. OW Kolejarz bez zbędnej zwłoki zawiadamia Osobę o naruszeniu ochrony Danych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej Osoby.

20. Żądania Osób.

1. **Prawa osób trzecich.** Realizując prawa Osób, których Dane dotyczą, OW Kolejarz wprowadza proceduralne 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 itp.), OW Kolejarz może zwrócić się do danej Osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.
2. **Nieprzetwarzanie.** OW Kolejarz informuje Osobę o tym, że nie przetwarza Danych jej dotyczących, jeśli taka Osoba zgłosiła żądanie dotyczące jej praw.

3. **Odmowa.** OW Kolejarz informuje Osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach Osoby z tym związanych.
4. **Dostęp do Danych.** Na żądanie Osoby dotyczące dostępu do jej Danych, OW Kolejarz informuje Osobę, czy przetwarza jej Dane oraz informuje Osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu Danych), a także udziela Osobie dostępu do Danych jej dotyczących. Dostęp do Danych może być zrealizowany przez wydanie kopii Danych, z zastrzeżeniem, że kopii Danych wydanej w wykonaniu prawa dostępu do Danych, OW Kolejarz a nie uzna za pierwszą nieodpłatną kopię Danych dla potrzeb opłat za kopie Danych.
5. **Kopie Danych.** Na żądanie OW Kolejarz wydaje osobie kopię Danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii Danych. OW Kolejarz wprowadza i utrzymuje cennik kopii Danych, zgodnie z którym pobiera opłaty za kolejne kopie Danych. Cena kopii Danych skalkulowana jest w oparciu o oszacowany jednostkowy koszt obsługi żądania wydania kopii Danych.
6. **Sprostowanie Danych.** OW Kolejarz dokonuje sprostowania nieprawidłowych Danych na żądanie Osoby. OW Kolejarz ma prawo odmówić sprostowania Danych, chyba że Osoba w rozsądny sposób wykaże nieprawidłowości Danych, których sprostowania się domaga. W przypadku sprostowania Danych OW Kolejarz informuje Osobę o odbiorcach Danych, na żądanie tej Osoby.
7. **Uzupełnienie Danych.** OW Kolejarz uzupełnia i aktualizuje Dane na żądanie Osoby. OW Kolejarz a ma prawo odmówić uzupełnienia Danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania Danych (np. OW Kolejarz nie musi przetwarzać Danych, które są OW Kolejarz zbędne). OW Kolejarz może polegać na oświadczeniu Osoby, co do uzupełnianych Danych, chyba że będzie to niewystarczające w świetle przyjętych przez OW Kolejarz procedur (np. co do pozyskiwania takich Danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.
8. **Usunięcie Danych.** Na żądanie Osoby, OW Kolejarz usuwa Dane, gdy:
 - a) Dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,
 - b) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
 - c) Osoba wniosła skuteczny sprzeciw względem przetwarzania tych Danych,
 - d) Dane były przetwarzane niezgodnie z prawem,
 - e) konieczność usunięcia Danych 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).

OW Kolejarz określa sposób obsługi prawa do usunięcia Danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony Danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art.17 ust.3 RODO. Jeżeli dane podlegające usunięciu zostały upublicznione przez OW Kolejarz, OW Kolejarz 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 OW Kolejarz informuje Osobę o odbiorcach Danych, na żądanie tej Osoby.

9. **Ograniczenie przetwarzania.** OW Kolejarz dokonuje ograniczenia przetwarzania Danych 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 dotyczą, sprzeciwia się usunięciu Danych Osobowych, żądając w zamian ograniczenia ich wykorzystywania,
 - c) OW Kolejarz 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 OW Kolejarz zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

W trakcie ograniczenia przetwarzania OW Kolejarz przechowuje Dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody Osoby, której Dane 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. OW Kolejarz informuje Osobę przed uchYLENIEM ograniczenia przetwarzania. W przypadku ograniczenia przetwarzania danych OW Kolejarz informuje Osobę o odbiorcach Danych, na żądanie tej Osoby.

10. **Przenoszenie danych.** Na żądanie Osoby OW Kolejarz 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 OW Kolejarz, przetwarzane na podstawie zgody tej Osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych OW Kolejarz.
11. **Sprzeciw w szczególnej sytuacji.** Jeżeli Osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej Danych, a Dane przetwarzane są przez OW Kolejarz w oparciu o uzasadniony interes OW Kolejarz lub o powierzone OW Kolejarz zadanie w interesie publicznym, OW Kolejarz uwzględni sprzeciw, o ile nie zachodzą po stronie OW Kolejarz ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.
12. **Sprzeciw przy badaniach naukowych, historycznych lub celach statystycznych.** Jeżeli OW Kolejarz prowadzi badania naukowe, historyczne lub przetwarza Dane w celach statystycznych, Osoba może wnieść umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania. OW Kolejarz uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

13. **Sprzeciw względem marketingu bezpośredniego.** Jeżeli Osoba zgłosi sprzeciw względem przetwarzania jej Danych przez OW Kolejarcz na potrzeby marketingu bezpośredniego (w tym ewentualnie profilowania), OW Kolejarcz uwzględni sprzeciw i zaprzestanie takiego przetwarzania.
14. **Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu.** Jeżeli OW Kolejarcz przetwarza dane 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, OW Kolejarcz zapewnia możliwość odwołania się do interwencji i decyzji człowieka po stronie OW Kolejarcz, chyba że taka automatyczna decyzja:
 - a) jest niezbędna do zawarcia lub wykonania umowy między odwołującą się Osobą a OW Kolejarcz,
lub
 - b) jest wprost dozwolona przepisami prawa,
lub
 - c) opiera się o wyraźną zgodę odwołującej Osoby.

21. Minimalizacja.

OW Kolejarcz dba o minimalizację przetwarzania Danych pod kątem:

- a) adekwatności Danych do celów (ilości danych i zakresu przetwarzania),
- b) dostępu do Danych,
- c) czasu przechowywania Danych.

22. Minimalizacja zakresu.

OW Kolejarcz zweryfikował zakres pozyskiwanych Danych, zakres ich przetwarzania i ilość przetwarzanych Danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO. OW Kolejarcz dokonuje okresowego przeglądu ilości przetwarzanych Danych i zakresu ich przetwarzania nie rzadziej niż raz na rok. OW Kolejarcz przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania Danych w ramach procedur zarządzania zmianą (*privacy by design*).

23. Minimalizacja dostępu.

1. OW Kolejarcz stosuje ograniczenia dostępu do Danych Osobowych:

- a) prawne (zobowiązania do poufności, zakresy upoważnień),
- b) fizyczne (strefy dostępu, zamykanie pomieszczeń),
- c) logiczne (ograniczenia uprawnień do systemów przetwarzających Dane Osobowe i zasobów sieciowych, w których rezydują Dane Osobowe).

2. OW Kolejarcz stosuje kontrolę dostępu fizycznego.

3. OW Kolejarcz dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających.

4. OW Kolejarcz 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 OW Kolejarcz.

24. Minimalizacja czasu.

1. OW Kolejarz wdraża mechanizmy kontroli cyklu życia Danych Osobowych w OW Kolejarz, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze.
2. Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów informatycznych OW Kolejarz, jak też z dokumentów papierowych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Spółkę. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia Danych, a w tym wymogi usuwania Danych.

25. Bezpieczeństwo. OW Kolejarz zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez OW Kolejarz.

26. Analizy ryzyka i adekwatności środków bezpieczeństwa.

1. OW Kolejarz przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa Danych Osobowych. W tym celu:
 - a) OW Kolejarz zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania – wewnątrz lub ze wsparciem podmiotów wyspecjalizowanych,
 - b) OW Kolejarz kategoryzuje Dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają,
 - c) OW Kolejarz przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania Danych lub ich kategorii. OW Kolejarz 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) OW Kolejarz ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym OW Kolejarz ustala przydatność i stosuje takie środki i podejście jak:
 - (i) pseudonimizacja,
 - (ii) szyfrowanie Danych Osobowych,
 - (iii) inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
 - (iv) 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.

27. Oceny skutków dla ochrony Danych.

OW Kolejarz dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony Danych Osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności Osób jest wysokie. OW Kolejarz stosuje metodykę oceny skutków przyjętą w OW Kolejarz.

28. Środki bezpieczeństwa.

OW Kolejarz stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony Danych. Środki bezpieczeństwa Danych Osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa w OW Kolejarz i są bliżej opisane w procedurach przyjętych przez OW Kolejarz dla tych obszarów.

29. Zgłaszanie naruszeń.

OW Kolejarz stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony Danych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia.

30. Przetwarzający.

OW Kolejarz posiada zasady doboru i weryfikacji przetwarzających Dane na rzecz OW Kolejarz opracowane 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 spoczywających na OW Kolejarz. OW Kolejarz przyjął minimalne wymagania co do umowy powierzenia przetwarzania Danych stanowiące Załącznik nr 2 do Polityki – „Wzór umowy powierzenia przetwarzania Danych”. OW Kolejarz rozlicza przetwarzających z wykorzystania podprzetwarzających, jak też z innych wymagań wynikających z Zasad powierzenia Danych Osobowych.

31. Eksport Danych.

OW Kolejarz rejestruje w Rejestrze przypadki eksportu Danych, czyli przekazywania Danych poza Europejski Obszar Gospodarczy (EOG w 2017 r. = Unia Europejska, Islandia, Lichtenstein i Norwegia). Aby uniknąć sytuacji nieautoryzowanego eksportu Danych w szczególności w związku z wykorzystaniem publicznie dostępnych usług chmurowych (shadow IT), OW Kolejarz okresowo weryfikuje zachowania użytkowników oraz w miarę możliwości udostępnia zgodne z prawem ochrony Danych rozwiązania równoważne.

32. Projektowanie Prywatności.

OW Kolejarz 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 OW Kolejarz odwołują się do zasad bezpieczeństwa Danych Osobowych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę Danych, uwzględnienia i zaprojektowana bezpieczeństwa i minimalizacji przetwarzania Danych od początku projektu lub inwestycji.