POLITYKA
OCHRONY DANYCH OSOBOWYCH

CAR HELP SP. Z O.O.

1. Niniejszy dokument zatytułowany "**Polityka Ochrony Danych Osobowych Car Help Sp. z o.o.**" (dalej jako **Polityka**) ma za zadanie stanowić wykaz wymogów, zasad i regulacji ochrony danych osobowych w Car Help Sp. z o.o. z siedzibą przy ulicy Towarowej 20B, 10-417 Olsztyn, reprezentowanej przez Zarząd (dalej także jako "Administrator", „Spółka" lub "ADO").

2. Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO - Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 lub RODO) (Dz.Urz. UE L 119, s. 1).

3. Polityka zawiera w szczególności opis zasad ochrony danych osobowych obowiązujących w Car Help Sp. z o.o., zwanej dalej "Spółką".

4. Niniejszy dokument stanowi najwyższej rangi dokument Polityki Ochrony Danych Osobowych w Spółce.

5. Z systemów przetwarzania danych osobowych znajdujących się w posiadaniu ADO mogą korzystać również inne podmioty, na podstawie odrębnych umów, porozumień lub stosunków prawnych, kształtowanych na podstawie przepisów szczególnych, określających zasady korzystania z tych systemów, w szczególności poprzez wyraźne zdefiniowanie celu i zakresu takiego korzystania oraz wskazanie odpowiedzialności karnej.

6. Skróty i definicje

Polityka oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu.

RODO oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1).

Administrator danych oznacza osobę fizyczną lub prawną, podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Administratorem danych jest Car Help Sp. z o.o.

Bezpieczeństwo informacji oznacza zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;

Dane osobowe oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); 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 szczególne 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;

Hasło oznacza ciąg znaków alfanumerycznych, znany jedynie użytkownikowi;

Identyfikator oznacza ciąg znaków literowych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

Incydent ochrony danych osobowych oznacza zdarzenie albo seria niepożądanych lub niespodziewanych zdarzeń ochrony danych osobowych stwarzających znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrożenia ochrony danych osobowych.

Naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Odbiorca danych oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią; organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

Osoba, podmiot danych oznacza osobę, której dane dotyczą;

Podmiot przetwarzający oznacza organizację lub osobę, której ADO powierzył przetwarzanie danych osobowych;

Postępowanie z ryzykiem oznacza proces planowania i wdrażania działań wpływających na ryzyko; Ryzyko – niepewność osiągnięcia zamierzonych celów;

Poufność danych oznacza właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom; szacowanie ryzyka – proces identyfikowania, analizowania i oceniania ryzyka;

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;

RCPDO lub rejestr oznacza rejestr czynności przetwarzania danych osobowych.

Serwisant oznacza firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego;

System informatyczny administratora danych oznacza sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych;

Teletransmisja oznacza przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;

Uwierzytelnienie oznacza działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

Użytkownik oznacza osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło;

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.

PUODO - Prezes Urzędu Ochrony Danych Osobowych.

Informacje - treści wszelkiego rodzaju przechowywane na dowolnym nośniku informacji, w postaci tradycyjnej - dokumentacja papierowa jak i elektronicznej - układy elektroniczne oraz inne nośniki, np. magnetyczne lub optyczne. Informacja może być wyrażona za pomocą mowy, pisma, obrazu, rysunku, znaku, kodu, dźwięku lub w jakikolwiek inny sposób.

7. Zasady ochrony danych.

ADO przetwarza dane osobowe z poszanowaniem następujących zasad:

1) w oparciu o podstawę prawną i zgodnie z prawem (**legalizm**);
2) rzetelnie i uczciwie (**rzetelność**);
3) w sposób przejrzysty dla osoby, której dane dotyczą (**transparentność**);
4) w konkretnych celach i nie "na zapas" (**minimalizacja**);
5) nie więcej niż potrzeba (**adekwatność**);
6) z dbałością o prawidłowość danych (**prawidłowość**);
7) nie dłużej niż potrzeba (**czasowość**);
8) zapewniając odpowiednie bezpieczeństwo danych (**bezpieczeństwo**).

8. ADO przetwarzając dane zapewnia:
   1) rozliczalność – rozumie się przez to właściwość zapewniającą, że działania użytkownika mogą być przypisane w sposób jednoznaczny tylko temu użytkownikowi;
   2) integralność danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   3) poufność danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;

4) integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej jak i przypadkowej.

9. Za przestrzeganie zasad ochrony i bezpieczeństwa danych odpowiedzialni są użytkownicy.

10. System ochrony danych

System ochrony danych osobowych w Spółce składa się z następujących elementów:

1) **Inwentaryzacja danych.** ADO dokonuje cyklicznej identyfikacji zasobów danych osobowych w Spółce, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania ewentualnych danych (inwentaryzacja), w tym:
   a) przypadków ewentualnego przetwarzania danych wrażliwych (**dane wrażliwe**);
   b) przypadków przetwarzania danych osób, których ADO nie identyfikuje (**dane niezidentyfikowane**);
   c) przypadków przetwarzania danych dzieci;
   d) profilowania;
   e) współadministrowania danymi.
2) **Rejestr.** ADO opracowuje, prowadzi i utrzymuje Rejestr Czynności Danych Osobowych w Spółce (Rejestr). Rejestr jest narzędziem rozliczania zgodności z ochroną danych w Spółce.
3) **Podstawy prawne.** ADO zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych.
4) **Obsługa praw jednostki.** ADO spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
   a) **Obowiązki informacyjne.** ADO przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków.
   b) **Możliwość wykonania żądań.** ADO weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających.
   c) **Obsługa żądań.** ADO zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO i dokumentowane.
   d) **Zawiadamianie o naruszeniach.** ADO stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.
5) **Minimalizacja.** ADO stosuje zasady i metody zarządzania minimalizacją (*privacy by default*), a w tym:
   a) zasady zarządzania **adekwatnością** danych;
   b) zasady reglamentacji i zarządzania **dostępem** do danych;
   c) zasady zarządzania okresem **przechowywania** danych i weryfikacji dalszej przydatności;
6) **Bezpieczeństwo.** ADO zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:
   a) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;
   b) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;
   c) dostosowuje środki ochrony danych do ustalonego ryzyka;
   d) posiada system zarządzania bezpieczeństwem informacji;
   e) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych − zarządza incydentami.

7) **Przetwarzający.** ADO stosuje zasady doboru przetwarzających dane na rzecz Spółki, wymogów co do warunków przetwarzania (umowa powierzenia), zasady weryfikacji wykonywania umów powierzenia.
8) **Eksport danych.** ADO ocenia, czy Spółka 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.
9) ***Privacy by design*.** ADO zarządza zmianami mającymi wpływ na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji w Spółce 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.
10) **Przetwarzanie transgraniczne.** ADO posiada zasady weryfikacji, kiedy zachodzą przypadki przetwarzania transgranicznego oraz zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO.

11. **Inwentaryzacja**

Dane wrażliwe
ADO identyfikuje ewentualne przypadki, w których przetwarza lub może przetwarzać dane wrażliwe (dane specjalne) oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania danych wrażliwych. W przypadku zidentyfikowania przypadków przetwarzania danych wrażliwych, ADO postępuje zgodnie z przyjętymi zasadami w tym zakresie.
Dane niezidentyfikowane
ADO identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane.
Profilowanie
ADO 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, ADO postępuje zgodnie z przyjętymi zasadami w tym zakresie.
Współadministrowanie
ADO identyfikuje przypadki współadministrowania danymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami.

12. **Rejestr Czynności Przetwarzania Danych**

- RCPD 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.
- ADO prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.
- RCPD jest jednym z podstawowych narzędzi umożliwiających ADO rozliczanie większości obowiązków ochrony danych.
- W Rejestrze, dla każdej czynności przetwarzania danych, którą ADO uznał za odrębną dla potrzeb Rejestru, ADO odnotowuje co najmniej: (I) nazwę czynności, (II) cel przetwarzania, (III) opis kategorii osób, (IV) opis kategorii danych, (V) opis kategorii odbiorców danych (w tym przetwarzających), (VI) ogólny opis technicznych i organizacyjnych środków ochrony danych.

13. **MINIMALIZACJA**

ADO dba o minimalizację przetwarzania danych pod kątem: (I) adekwatności danych do celów (ilości danych i zakresu przetwarzania), (II) dostępu do danych, (III) czasu przechowywania danych.

a) Minimalizacja zakresu

ADO zweryfikował zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO.

ADO dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.

ADO przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (*privacy by design*).

b) Minimalizacja dostępu

ADO stosuje ograniczenia dostępu do danych osobowych: prawne (zobowiązania do poufności, zakresy upoważnień), logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe).

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

ADO dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.

c) **Minimalizacja czasu**

Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów Spółki. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez ADO.

14. **PRZETWARZAJĄCY**

- ADO dba, aby przetwarzający dawali wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na ADO.

- ADO rozlicza przetwarzających z wykorzystania podprzetwarzających, jak też z innych wymagań wynikających z powierzenia danych osobowych.

15. **PROJEKTOWANIE PRYWATNOŚCI**

ADO 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 ADO 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.

16. **Sposób obsługi praw jednostki i obowiązków informacyjnych**

- ADO dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.
- ADO dba o dotrzymywanie prawnych terminów realizacji obowiązków względem

osób.
- ADO wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.
- W celu realizacji praw jednostki ADO zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez ADO zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany,
- ADO dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

a) Obowiązki informacyjne

- ADO określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.
- ADO informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.
- ADO informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.
- ADO informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej.
- ADO informuje osobę o planowanej zmianie celu przetwarzania danych.
- ADO informuje osobę przed uchyleniem ograniczenia przetwarzania.
- ADO informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).
- ADO informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.
- ADO bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

b) Żądania osób

Prawa osób trzecich. Realizując prawa osób, których dane dotyczą, ADO 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.), ADO może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.
Nieprzetwarzanie. ADO informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.
Odmowa. ADO informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.
Dostęp do danych. Na żądanie osoby dotyczące dostępu do jej danych, ADO 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 ADO nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.

Kopie danych. Na żądanie ADO wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych.
Sprostowanie danych. ADO dokonuje sprostowania nieprawidłowych danych na żądanie osoby. ADO ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych ADO informuje osobę o odbiorcach danych, na żądanie tej osoby.
Uzupełnienie danych. ADO uzupełnia i aktualizuje dane na żądanie osoby. ADO ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. ADO nie musi przetwarzać danych, które są ADO zbędne). ADO może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez ADO procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.
Usunięcie danych. Na żądanie osoby, ADO usuwa dane, gdy:

1) dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,
2) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
3) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
4) dane były przetwarzane niezgodnie z prawem,
5) konieczność usunięcia wynika z obowiązku prawnego,
6) 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).

   ADO 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 Spółkę, ADO 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 ADO informuje osobę o odbiorcach danych, na żądanie tej osoby.

Ograniczenie przetwarzania. ADO 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) ADO 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 ADO zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

W trakcie ograniczenia przetwarzania ADO 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.

ADO informuje osobę przed uchyleniem ograniczenia przetwarzania.

W przypadku ograniczenia przetwarzania danych ADO informuje osobę o odbiorcach

danych, na żądanie tej osoby.

Przenoszenie danych. Na żądanie osoby ADO 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 ADO, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych ADO.

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

Dostęp do danych osobowych:

1) Przetwarzanie, w tym udostępnianie danych osobowych jest prawnie dopuszczalne, jeżeli jest niezbędne dla zrealizowania obowiązku wynikającego z przepisu prawa.
2) W przypadku udostępnienia danych osobowych w celach innych niż włączenie do rejestru, administrator danych udostępnia posiadane informacje osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
3) Dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
4) Podmiot występujący o udostępnienie informacji powinien wskazać podstawę prawną upoważniającą go do otrzymania tych danych albo uzasadnioną potrzebę żądania ich udostępnienia. Tylko w takiej sytuacji można dokonać oceny, czy w określonym przypadku udostępnienie danych jest prawnie dopuszczalne i czy nie będzie ono stanowić naruszenia zasad ochrony informacji.
5) Przetwarzanie, w tym udostępnianie danych osobowych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą, oraz następuje w celu badań naukowych, dydaktycznych, historycznych oraz statystycznych.
6) Udostępnienie danych może nastąpić jedynie za zgodą Administratora danych i powinno być odpowiednio udokumentowane.

17. **BEZPIECZEŃSTWO**

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

a) Analizy ryzyka i adekwatności środków bezpieczeństwa

ADO przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:

1) ADO zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji i ciągłości działania − wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.
2) ADO kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.
3) ADO przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. ADO 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.

4) ADO ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym ADO może ustalić przydatność i stosować 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.

b) Oceny skutków dla ochrony danych

- ADO dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.

c) Środki bezpieczeństwa

ADO stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych.

W celu zwiększenia efektywności ochrony danych osobowych dokonano połączenia różnych zabezpieczeń w sposób umożliwiający stworzenie kilku warstw ochronnych. Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.

Realizację powyższych zamierzeń powinny zagwarantować następujące założenia:

1) Wdrożenie procedur określających postępowanie osób dopuszczonych do przetwarzania danych osobowych oraz ich odpowiedzialność za ochronę tych danych.
2) Przeszkolenie użytkowników w zakresie bezpieczeństwa i ochrony danych osobowych.
3) Przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła, identyfikatory).
4) Podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie zabezpieczeń,
5) Okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych.

Dla zapewnienia bezpieczeństwa danych i informacji zastosowano następujące środki organizacyjne:

1) Każda osoba działająca z upoważnienia Administratora i mająca dostęp do danych osobowych przetwarzała je wyłącznie na polecenie Administratora.
2) Każdy z pracowników i współpracowników powinien zachować szczególną ostrożność przy przenoszeniu danych.
3) Należy chronić dane przed dostępem do nich osób nieupoważnionych.
4) Pomieszczenia w których są przetwarzane dane osobowe powinny być zamykane na klucz.
5) Dostęp do kluczy posiadają tylko upoważnieni pracownicy i współpracownicy.

6) Dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy. W wypadku gdy jest wymagany poza godzinami pracy – możliwy jest tylko na podstawie zezwolenia Administratora.
7) Dostęp do pomieszczeń, w których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy.
8) W przypadku pomieszczeń, do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności.
9) Szafy, w których przechowywane są dane powinny być zamykane na klucz.
10) Klucze do tych szaf posiadają tylko upoważnieni pracownicy.
11) Szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych, a następnie powinny być zamykane.
12) Dane w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych, a następnie muszą być chowane do szaf.
13) Dostęp do komputerów, na których są przetwarzane dane - mają tylko upoważnieni pracownicy i współpracownicy.
14) Monitory komputerów, na których przetwarzane są dane, są tak ustawione, aby osoby nieupoważnione nie miały wglądu w dane.
15) W wypadku potrzeby wyniesienia komputera przenośnego (np. typu notebook) zawierającego dane osobowe, lub inne informacje chronione, komputer taki musi być odpowiednio dodatkowo zabezpieczony, a dane zaszyfrowane.
16) Nie wolno udostępniać osobom nieupoważnionym tych komputerów.
17) W przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami - należy dokonać tego z zachowaniem szczególnej ostrożności.
18) Nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie), aby nie zostały na nich dane osobowe.
19) W wypadku niemożliwości skasowania danych z nośnika (płyta CD-ROM) - należy taką płytę zniszczyć fizycznie.
20) W przypadku wykorzystania do przenoszenia dysków - dane należy kasować z tych dysków.
21) Niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną.
22) Sieć komputerowa powinna być zabezpieczona przed wszelkim dostępem z zewnątrz.
23) Błędne lub nieaktualne wydruki i wersje papierowe zawierające dane osobowe lub inne informacje chronione - niszczone są za pomocą niszczarki lub w inny mechaniczny sposób uniemożliwiający powtórne ich odtworzenie.

d) Zgłaszanie naruszeń

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

1. Za naruszenie ochrony danych osobowych uważa się w szczególności:
   1) nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują
   2) naruszenie lub próby naruszenia integralności danych rozumiane jako wszelkie modyfikacje, zniszczenia lub próby ich dokonania przez osoby nieuprawnione lub uprawnione działające w złej wierze lub jako błąd w działaniu osoby uprawnionej (np. zmianę zawartości danych, utratę całości lub części danych),
   3) naruszenie lub próby naruszenia integralności systemu

4) zmianę lub utratę danych zapisanych na kopiach zapasowych,
5) naruszenie lub próby naruszenia poufności danych,
6) nieuprawniony dostęp (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu),
7) udostępnienie osobom nieupoważnionym danych osobowych
8) zniszczenie, uszkodzenie lub wszelkie próby nieuprawnionej ingerencji w system informatyczny zmierzające do zakłócenia jego działania bądź pozyskania w sposób niedozwolony lub w celach niezgodnych z przeznaczeniem danych zawartych w systemie,
9) inny stan systemu informatycznego lub pomieszczeń, niż pozostawiony przez użytkownika po zakończeniu pracy.

2. Za naruszenie ochrony danych osobowych uważa się również włamanie do budynku lub pomieszczeń, w których przetwarzane są dane osobowe lub próby takich działań.

3. W przypadku stwierdzenia naruszenia:
1) zabezpieczenia systemu informatycznego,
2) technicznego stanu urządzeń,
3) zawartości zbioru danych osobowych,
4) ujawnienia metody pracy lub sposobu działania programu,
5) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
6) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.) każda osoba zatrudniona przy przetwarzaniu danych jest obowiązana niezwłocznie powiadomić o tym fakcie Administratora danych.

4. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne lub porządkowe.
Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych.

18. Polityka jest dokumentem wewnętrznym i nie może być udostępniana osobom postronnym w żadnej formie.

19. Użytkownicy są zobowiązani zapoznać się z treścią Polityki.

20. Użytkownik zobowiązany jest złożyć oświadczenie o tym, iż został zaznajomiony z przepisami ustawy o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych, z niniejszą Polityką, a także zobowiązać się do ich przestrzegania.

21. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie aktualnie obowiązujące przepisy prawa w zakresie ochrony danych osobowych.

22. Użytkownicy zobowiązani są do bezwzględnego stosowania przy przetwarzaniu danych postanowień zawartych w niniejszej Polityce. W wypadku odrębnych od zawartych w niniejszej Polityce uregulowań występujących w innych procedurach obowiązujących u Administratora Danych, użytkownicy mają obowiązek stosowania unormowań dalej idących, których stosowanie zapewni wyższy poziom ochrony informacji.