Broszura informacyjna przetwarzanie danych osobowych w AWL

Prawidłowe przetwarzanie danych osobowych jest dla AWL sprawą wysokiej wagi, a ich ochronę Akademia traktuje z należytą starannością zapewniając pełne ich bezpieczeństwo. W związku z tym, że ochrona danych osobowych jest rozległym i specjalistycznym obszarem chcemy dostarczyć Państwu zestaw skróconych informacji o tym, dlaczego i w jakim celu przetwarzamy dane osobowe w AWL, jakie są główne zasady wynikające z RODO w związku z ich przetwarzaniem oraz wszelkich innych informacji w tym zakresie, które mogą być dla Państwa istotne. Pragniemy zapewnić Państwa o tym, że AWL kładzie duży nacisk na przestrzeganie surowych zasad określających, które komórki organizacyjne lub które osoby funkcyjne mają dostęp do przetwarzanych danych osobowych oraz jakie dane osobowe mogą podlegać przetwarzaniu.

Prosimy o zapoznanie się z przygotowanymi informacjami dotyczącymi sposobu przetwarzania danych.

Wrocław 2021

1. Wstęp

RODO to inaczej Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 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 (inaczej ogólne rozporządzenie o ochronie danych osobowych - RODO). Wdrożenie RODO wynika po pierwsze z konieczności dostosowania przepisów do rozwoju technologii, a po drugie z potrzeby wprowadzenia jednolitych zasad ochrony danych osobowych we wszystkich państwach Unii Europejskiej.

2. Administrator Danych Osobowych

Administrator to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.
Administratorem danych osobowych jest Akademia Wojsk Lądowych imienia generała Tadeusza Kościuszki ul. Czajkowskiego 109, 51-147 Wrocław.

Administrator danych osobowych jest zobowiązany w szczególności do:

- zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochrona, 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,
- prowadzeniem dokumentacji opisującej sposób przetwarzania danych oraz środków informatyczno - technicznych,
- zapewnieniem kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane,
- zapewnieniem, że do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie, które ADO nadaje,
- prowadzeniem rejestru osób upoważnionych do przetwarzania danych osobowych,
- informowaniem osób, których dane dotyczą o adresie swojej siedziby, celu zbierania i przetwarzania danych, o odbiorcach tych danych oraz o prawie dostępu do danych i możliwości ich aktualizacji.

3. Inspektor Ochrony Danych

Inspektor Ochrony Danych Osobowych (IOD) to osoba powoływana przez Administratora lub podmiot przetwarzający do pomocy przy przestrzeganiu w firmie lub organizacji przepisów o ochronie danych osobowych. IOD pełni rolę pośrednika pomiędzy zainteresowanymi podmiotami (Urzędem Ochrony Danych Osobowych, podmiotem przetwarzającym dane oraz

osobą, której dane są przetwarzane). Ponadto IOD zapewnia realizację zasady rozliczalności - pomaga przy sporządzaniu oceny ryzyka, czy oceny skutku ochrony danych osobowych.

Kluczowe zadania Inspektora Ochrony Danych Osobowych to:

- informowanie Administratora, podmiotu przetwarzającego oraz pracowników o obowiązkach w zakresie ochrony danych osobowych wynikających z RODO,
- doradzanie, jak przestrzegać przepisów o ochronie danych osobowych,
- monitorowanie przestrzegania przepisów i polityk w zakresie ochrony danych osobowych,
- pomaganie przy sporządzaniu oceny ryzyka lub oceny skutków dla ochrony danych osobowych,
- zachowanie poufności względem wykonywanych zadań w ramach ochrony danych osobowych,
- pełnienie funkcji punktu kontaktowego dla organu nadzorczego.

Administrator wyznaczył inspektora ochrony danych osobowych. Można się z nim skontaktować w następujący sposób:

- listownie na adres: Inspektor Ochrony Danych, 51-147 Wrocław, ul. Czajkowskiego 109,
- przez e-mail: iod@awl.edu.pl
- telefonicznie pod numer 261-658-474

4. Dane osobowe i kategorie przetwarzanych danych w AWL

Dane osobowe to informacje o osobie fizycznej takie jak: imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczegółów określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Szczególna kategoria danych osobowych dane wrażliwe, czyli dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej osoby fizycznej.

AWL przetwarza następujące kategorie danych:

- dane kandydatów na żołnierzy zawodowych,
- dane studentów i słuchaczy kursów ,
- dane żołnierzy pełniących służbę,
- dane osób zatrudnionych,
- dane kontrahentów, zleceniobiorców itp.
- dane wnioskodawców w celu rozpatrzenia sprawy i udzielenia odpowiedzi także w spawach skarg i wniosków,
- dane innych kategorii osób wynikające z przepisów prawa.

5. Cele i podstawy prawne przetwarzania danych

W Akademii, przetwarzane są dane wynikające z realizacji zadań statutowych i przepisów prawa:

- w celu wypełnienia obowiązku prawnego, który ciąży na organie administracji publicznej (art. 6 ust. 1 lit. c RODO),
- w celu realizacji zawartych umów (art 6 ust. 1 lit. b RODO),
- w celu wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej (9 ust.1 lit. b RODO),
- w celach zapobiegania rozprzestrzeniania się chorób zakaźnych w tym monitorowania epidemii i ich rozprzestrzeniania się COVID-19 w związku z zaleceniami i wytycznymi WOMP (art. 9 ust.1 lit. b RODO, art. 6 ust. 1 lit e RODO),
- w celu podjęcia działań na żądanie osoby której dane dotyczą (6 ust. 1 lit. b RODO),
- na podstawie zgody osoby na przetwarzanie danych osobowych (art. 6 ust. 1 lit a RODO),
- w celu ustalenia, dochodzenie lub obrony roszczeń w postępowaniu sądowym, administracyjnym lub też innym postępowaniu pozasądowym (art. 6 ust. 1 lit d RODO),
- w zakresie działania w mediach społecznościowych, kontaktu z użytkownikami, informowania o aktywności administratora (art. 6 ust. 1 lit f RODO),
- w celu prowadzenia monitoringu wizyjnego (art. 6 ust. 1 lit f RODO),
- w celu prowadzenia korespondencji (art. 6 ust. 1 lit e RODO).

6. Główne zasady przetwarzania danych

Zasada przejrzystości, rzetelności i legalności (zgodności z prawem)

Administrator jest zobowiązany podczas obowiązku informacyjnego używać formy zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej oraz informowania w sposób jasny oraz prostym językiem.

Zasada celowości

Zgodnie z tą zasadą należy przetwarzać dane osobowe zgodnie z konkretnym, wyraźnym i prawnie uzasadnionym celem. Cel zbierania danych osobowych powinien być określony wyraźnie i konkretnie i należy przy tym unikać ogólnikowych celów przetwarzania. Zasada ta łączy się z obowiązkiem informacyjnym - informowanie administratora osoby, której dane dotyczą o celu przetwarzania danych osobowych.

Zasada minimalizacji danych

Zgodnie z tą zasadą przetwarzane dane powinny być adekwatne, stosowne i ograniczone do osiągnięcia założonego celu. Oznacza to, aby pozyskiwać takie dane, które będą konieczne do osiągnięcia zamierzonego celu. Przykładem może być zawarcie umowy sprzedaży zawieranej w formule na odległość. Niezbędnymi danymi do realizacji tej umowy

będą: imię, nazwisko, adres zamieszkania czy niekiedy numer telefonu. Wyżej wymienione dane będą w zupełności wystarczające do realizacji tej umowy. Zbędne wydaje się w tej sytuacji być wymaganie od drugiej osoby, np. wieku, wykształcenia czy też formy spędzania czasu.

Zasada prawidłowości

Zgodnie z tą zasadą przetwarzane dane powinny być adekwatne, stosowne i ograniczone do osiągnięcia założonego celu. Oznacza to, aby pozyskiwać takie dane, które będą konieczne do osiągnięcia zamierzonego celu. Przykładem może być zawarcie umowy sprzedaży zawartej na odległość. Niezbędnymi danymi do realizacji tej umowy będą: imię, nazwisko, adres zamieszkania czy niekiedy numer telefonu. Wyżej wymienione dane będą w zupełności wystarczające do realizacji tej umowy. Zbędne wydaje się w tej sytuacji być wymaganie od drugiej osoby, np. wieku, wykształcenia czy też formy spędzania czasu.

Zasada ograniczenia przetwarzania

Zgodnie z tą zasadą dane osobowe powinny być przechowywane przez okres nie dłuższy niż jest to konieczne uzyskania celów, w których dane te były przetwarzane. Przykładem może być prowadzenie rachunku bankowego. Po osiągnięciu celu (moment zamknięcia rachunku bankowego) przetwarzanie danych osoby, która posiadała rachunek bankowy należałoby uznać za nielegalne.

Zasada integralności i poufności (bezpieczeństwa danych)

Zasada ta nakłada obowiązek na Administratora danych przetwarzania danych w sposób, który zapewni ich bezpieczeństwo podczas przetwarzana. Bezpieczeństwo danych to ich ochrona przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem, a także uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

Zasada rozliczalności

Administrator danych jest odpowiedzialny za przestrzeganie powyższych zasad i musi być w stanie wykazać ich przestrzeganie.

7. Naruszenia ochrony danych i sposób postępowania

Naruszenie ochrony danych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem:

- zniszczenia danych osobowych,
- utracenia danych osobowych,
- zmodyfikowania danych osobowych,
- nieuprawnionego ujawnienia danych osobowych,
- nieuprawnionego dostępu do danych osobowych.

Klasyfikacja naruszeń:

- umyślne incydenty (np. kradzież danych i sprzętu, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie danych, włamanie do systemu informatycznego lub pomieszczeń),
- zdarzenia losowe wewnętrzne (np. awaria komputera/serwera/dysku twardego/oprogramowania, pomyłki informatyków, utrata danych),
- zdarzenia losowe zewnętrzne (np. pożar, zalanie wodą, utrata zasilania, utrata łączności).

Uproszczona procedura postępowania w przypadku naruszeń:

- niezwłocznie zgłosić do IOD lub przełożonego,
- opisać przyczyny i możliwe skutki incydentu,
- wdrożyć środki zabezpieczające,
- sporządzić raport,
- zawiadomić organ nadzorczy,
- zawiadomić osoby, której dane dotyczą.

8. Środki organizacyjne i techniczne ochrony danych

Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

Przestrzegając kluczowych zasad RODO zastosuj się do:

- zachowania poufności przetwarzanych danych,
- dane osobowe wykorzystuj wyłącznie do celów, dla których zostały udostępnione,
- dokumenty zawierające informacje podlegające ochronie przechowuj na biurku i w innych miejscach do tego przeznaczonych, w taki sposób, aby osoba nieuprawniona nie miała do nich dostępu,
- nośników informacji (w formie papierowej i elektronicznej) z danymi podlegającymi ochronie nie pozostawiaj w miejscach ogólnodostępnych i niezabezpieczonych oraz nie udostępniaj osobom nieupoważnionym,
- dokumenty wydrukowane w nadmiernej ilości, a także zawierające błędy lub, które nie są wykorzystywane do żadnych celów trwale zniszcz w sposób uniemożliwiający odtworzenie treści,
- używaj identyfikatorów i haseł i nie udostępniaj ich innym osobom, a w przypadku podejrzenia, że osoba postronna weszła w ich posiadanie, dokonaj ich zmiany zgodnie z obowiązującymi procedurami,
- loguj się do systemu pocztowego przy pomocy internetowej przeglądarki powinno być przeprowadzone na osobistym komputerze, laptopie posiadającym zabezpieczenie antywirusowe,
- stosuj hasła dostępowe do konta pocztowego i systemów informatycznych i chroń je przed dostępem osób trzecich,

- po zakończeniu pracy wyloguj się ze wszystkich systemów, z których korzystałeś,
- adres konta pocztowego udostępniaj i wykorzystuj wyłącznie w celach służbowych,
- monitor należy ustaw w taki sposób, aby osoby nieupoważnione wchodzące do pomieszczenia nie miały wglądu do danych na nim wyświetlanych,
- przed zalogowaniem się do systemu stacji roboczej upewnij się, że w pobliżu nie ma osób trzecich lub urządzeń nagrywających mogących zarejestrować hasła dostępowe do systemów, z których zamierzasz skorzystać.

Opracował:
INSPEKTOR OCHORNY DANYCH
mgr Joanna KUBIAK