

mChoroszczRP

Polityka prywatności

Zasady przetwarzania danych osobowych w mChoroszczRP

Wersja 1.0 | obowiązuje od 11 lipca 2026 r.

Kontakt z administracją

telefonicznie: 71 707 23 91

mailowo: kontakt@kubusekmeow.pl

Spis treści

1. Najważniejsze informacje
2. Administrator danych i kontakt
3. Zakres zastosowania polityki
4. Kategorie przetwarzanych danych
5. Dane otrzymywane z Google
6. Dane podawane przez użytkownika
7. Dane techniczne, cookies i logi
8. Cele i podstawy prawne przetwarzania
9. Czy podanie danych jest obowiązkowe
10. Odbiorcy i podmioty przetwarzające
11. Google, Discord, Roblox i ER:LC
12. Transfer danych poza Europejski Obszar Gospodarczy
13. Okres przechowywania danych
14. Bezpieczeństwo danych
15. Prawa użytkownika
16. Usunięcie konta i cofnięcie dostępu Google
17. Dane dzieci i osób niepełnoletnich
18. Profilowanie i decyzje automatyczne
19. Naruszenia ochrony danych
20. Zmiany polityki
21. Skrócona tabela przetwarzania
22. Podstawy prawne i informacje końcowe

1. Najważniejsze informacje

Polityka wyjaśnia, jakie dane osobowe są przetwarzane w związku z korzystaniem z mChoroszczRP, skąd pochodzą, w jakich celach są używane, komu mogą być ujawniane, jak długo są przechowywane oraz jakie prawa przysługują użytkownikowi.

mChoroszczRP korzysta z logowania Google. W zależności od konfiguracji i zakresu przyznanego przez użytkownika system otrzymuje z Google: unikalny identyfikator konta, adres e-mail, imię, nazwisko oraz zdjęcie profilowe. Dane te dotyczą prawdziwego konta OOC i są odrębne od fikcyjnych danych postaci IC.

System przetwarza także nick OOC, dane postaci RolePlay, nick Discord, nick Roblox, dane pojazdów i dokumentów RP, saldo i historię operacji RP, zgłoszenia, wpisy służbowe, logi działań, adres IP, informacje o przeglądarce, sesji i zdarzeniach bezpieczeństwa.

mChoroszczRP jest usługą RolePlay. Dane postaci IC, mandaty, wyroki i dokumenty RP są co do zasady danymi fikcyjnymi, jednak mogą stać się danymi osobowymi, jeżeli użytkownik umieści w nich informacje pozwalające zidentyfikować prawdziwą osobę.

2. Administrator danych i kontakt

Administratorem danych jest operator projektu mChoroszczRP działający pod nazwą KubusekMeow.

Kontakt w sprawach prywatności, realizacji praw, usunięcia konta, sprzeciwu, naruszenia bezpieczeństwa lub pytań dotyczących przetwarzania danych:

- telefon: 71 707 23 91;
- e-mail: kontakt@kubusekmeow.pl.

2.1. Inspektor ochrony danych

Jeżeli administrator wyznaczy inspektora ochrony danych, jego dane kontaktowe zostaną podane w systemie. Jeżeli inspektor nie został wyznaczony, wszystkie sprawy należy kierować bezpośrednio do administratora na wskazany adres e-mail.

2.2. Tożsamość osoby składającej wniosek

Administrator może poprosić o informacje potrzebne do potwierdzenia, że wniosek dotyczący danych składa właściwy użytkownik. Weryfikacja powinna być proporcjonalna i nie może prowadzić do zbierania nadmiarowych danych.

3. Zakres zastosowania polityki

Polityka dotyczy strony internetowej, panelu użytkownika, modułów administracyjnych i policyjnych RP, logowania Google, bazy SQLite, integracji ER:LC, webhooków Discord oraz innych funkcji mChoroszczRP.

Polityka nie zastępuje dokumentów prywatności Google, Discord, Roblox, ER:LC, dostawcy hostingu ani operatora sieci. Podmioty te mogą samodzielnie przetwarzać dane użytkownika zgodnie z własnymi zasadami.

Jeżeli mChoroszczRP jest wdrożony przez innego operatora na odrębnej domenie lub serwerze, administratorem danych może być ten operator. W takim przypadku powinien on dostosować dokument i podać własne dane kontaktowe, dostawców oraz okresy przechowywania.

4. Kategorie przetwarzanych danych

4.1. Dane identyfikacyjne i konta OOC

- unikalny identyfikator Google (np. wartość sub);
- adres e-mail Google i informacja o jego weryfikacji;
- imię i nazwisko z profilu Google;
- zdjęcie profilowe Google albo adres prowadzący do zdjęcia;
- nick OOC, rola, status konta, uprawnienia i data utworzenia;
- informacja o migracji starego konta do logowania Google.

4.2. Dane RolePlay

- imię, nazwisko i data urodzenia postaci IC;
- numer mieszkańca, status dokumentu i fikcyjne dokumenty RP;
- pojazdy, tablice RP, wirtualne licencje i przedmioty;
- saldo RP, przelewy, zakupy, mandaty i historia operacji;
- zgłoszenia, wpisy Policji RP, wyroki, listy gończe i status służby;
- historia Character Kill i działań administracyjnych.

4.3. Dane kontaktowe i integracyjne

- nick Discord podany przez użytkownika;
- nick Roblox używany do integracji ER:LC;
- treść zgłoszeń i kontakt RP podany dobrowolnie;
- identyfikatory potrzebne do obsługi webhooków i integracji, jeśli są włączone.

4.4. Dane techniczne

- adres IP, czas połączenia i identyfikatory sesji;
- typ przeglądarki, system operacyjny, język, rozdzielczość i ogólne informacje o urządzeniu;
- żądany adres, kod odpowiedzi, błędy, próby logowania i zdarzenia bezpieczeństwa;
- cookies niezbędne do utrzymania sesji, ochrony CSRF i ustawień interfejsu.

5. Dane otrzymywane z Google

Logowanie Google wykorzystuje standard uwierzytelniania OpenID Connect lub usługę Sign in with Google. Po wybraniu przycisku logowania użytkownik uwierzytelnia się w Google, a mChoroszczRP otrzymuje dane potrzebne do rozpoznania konta.

System pobiera i może przechowywać następujące dane z profilu Google: imię, nazwisko, adres e-mail, zdjęcie profilowe oraz unikalny identyfikator konta Google. Może również otrzymać informację, czy adres e-mail został zweryfikowany.

Imię, nazwisko i zdjęcie Google mogą być wyświetlane w profilu konta OOC, panelu administracyjnym lub jako element identyfikacji zalogowanego użytkownika. Nie są automatycznie przepisywane do fikcyjnej postaci IC, chyba że użytkownik sam wpisze takie dane w formularzu postaci.

Unikalny identyfikator Google jest podstawowym technicznym kluczem powiązania konta. Adres e-mail może się zmienić albo być inny w zależności od typu konta, dlatego samo porównanie e-maili nie zawsze powinno być jedyną metodą identyfikacji.

mChoroszczRP nie uzyskuje dostępu do treści Gmaila, Dysku Google, kontaktów, kalendarza ani hasła Google, jeżeli nie zostaną w przyszłości dodane odrębne zakresy uprawnień i wyraźnie opisane w zaktualizowanej polityce.

6. Dane podawane przez użytkownika

Po pierwszym logowaniu użytkownik podaje nick OOC i dane postaci IC. Może również podać nick Discord i Roblox. Dane te są wykorzystywane do prowadzenia konta, rozgrywki oraz działania integracji.

Użytkownik powinien podawać wyłącznie dane potrzebne. Pola fabularne nie powinny zawierać prawdziwego numeru PESEL, numeru dokumentu tożsamości, adresu, danych zdrowotnych, danych szkoły ani innych informacji szczególnie prywatnych.

Treść zgłoszeń, notatek policyjnych RP i logów może być widoczna dla administratorów lub osób pełniących odpowiednie role. Nie należy umieszczać tam informacji o rzeczywistych przestępstwach, ofiarach, zdrowiu, życiu seksualnym, poglądach politycznych ani innych szczególnych kategoriach danych.

Jeżeli użytkownik poda dane innej osoby, powinien mieć ku temu podstawę i ograniczyć zakres informacji. Administrator może usunąć dane osoby trzeciej po otrzymaniu wiarygodnego zgłoszenia.

7. Dane techniczne, cookies i logi

Przy każdym połączeniu serwer może automatycznie zapisywać dane techniczne potrzebne do dostarczenia strony, diagnozowania błędów i ochrony przed nadużyciami. Obejmują one adres IP, znacznik czasu, żądany zasób, przeglądarkę i wynik operacji.

Cookies sesyjne są używane do utrzymania zalogowania, rozpoznania sesji, ochrony formularzy przed atakami CSRF oraz zachowania niektórych ustawień interfejsu. Bez niezbędnych cookies logowanie i działanie panelu może być niemożliwe.

Jeżeli w przyszłości zostaną włączone cookies analityczne, reklamowe lub inne opcjonalne technologie, użytkownik powinien otrzymać odrębny mechanizm wyboru przed ich zapisaniem, chyba że prawo przewiduje wyjątek.

Logi administracyjne mogą obejmować informację o tym, kto i kiedy zmienił saldo, uprawnienia, dokument, pojazd, zgłoszenie lub status konta. Ich celem jest rozliczalność, bezpieczeństwo i możliwość odtworzenia przebiegu zdarzeń.

8. Cele i podstawy prawne przetwarzania

8.1. Utworzenie i prowadzenie konta

Dane Google, nick OOC, profil i sesja są przetwarzane w celu zawarcia i wykonywania umowy o świadczenie usługi elektronicznej - art. 6 ust. 1 lit. b RODO.

8.2. Prowadzenie rozgrywki

Dane postaci, dokumentów RP, pojazdów, banku, sklepu, zgłoszeń i służb są przetwarzane w celu wykonania usługi i realizacji funkcji wybranych przez użytkownika - art. 6 ust. 1 lit. b RODO.

8.3. Bezpieczeństwo i przeciwdziałanie nadużyciom

Adres IP, logi, próby logowania, historia uprawnień i działania administratorów są przetwarzane na podstawie prawnie uzasadnionego interesu administratora polegającego na ochronie systemu, użytkowników i możliwości dochodzenia roszczeń - art. 6 ust. 1 lit. f RODO.

8.4. Obsługa reklamacji i kontaktu

Dane przekazane w wiadomości lub rozmowie są przetwarzane w celu obsługi zgłoszenia, wykonania umowy albo realizacji prawnie uzasadnionego interesu w postaci udzielenia odpowiedzi i dokumentowania sprawy - art. 6 ust. 1 lit. b lub f RODO.

8.5. Obowiązki prawne

Dane mogą być przetwarzane, gdy jest to wymagane przepisem prawa, prawomocnym orzeczeniem lub żądaniem uprawnionego organu - art. 6 ust. 1 lit. c RODO.

8.6. Funkcje opcjonalne

Jeżeli określona funkcja, komunikacja lub publikacja zdjęcia wymaga odrębnej zgody, podstawą będzie art. 6 ust. 1 lit. a RODO. Zgodę można wycofać bez wpływu na zgodność wcześniejszego przetwarzania.

9. Czy podanie danych jest obowiązkowe

Podanie danych potrzebnych do logowania Google, utworzenia nicku i postaci jest dobrowolne, ale konieczne do korzystania z podstawowych funkcji. Brak tych danych uniemożliwia utworzenie konta lub prowadzenie rozgrywki.

Nick Discord i Roblox może być formalnie opcjonalny, jednak brak nicku Roblox może uniemożliwić działanie integracji ER:LC, a brak Discorda może utrudnić kontakt lub udział w modułach powiązanych z serwerem.

Podanie dodatkowych informacji w zgłoszeniu jest dobrowolne. Użytkownik powinien ograniczyć treść do danych koniecznych do opisanie zdarzenia RP.

Nie ma obowiązku podawania prawdziwych danych jako danych postaci IC. Wprost zaleca się używanie danych fikcyjnych.

10. Odbiorcy i podmioty przetwarzające

Dostęp do danych mogą otrzymać osoby upoważnione przez administratora: ROOT, administratorzy, moderatorzy, funkcjonariusze RP i dyżurni - wyłącznie w zakresie odpowiadającym ich roli.

Dane mogą być powierzane dostawcy hostingu, usług kopii zapasowej, poczty elektronicznej, ochrony przed atakami, monitorowania błędów i utrzymania technicznego. Powierzenie powinno opierać się na odpowiednich umowach i zabezpieczeniach.

Wybrane informacje mogą zostać przekazane Google w związku z logowaniem, Discord przez webhook, Roblox lub ER:LC w związku z integracją. Zakres zależy od włączonych funkcji i działań użytkownika.

Dane mogą zostać ujawnione uprawnionemu organowi publicznemu, sądowi lub innemu podmiotowi, jeżeli administrator ma prawny obowiązek ich przekazania. Administrator nie udostępnia danych reklamodawcom i nie sprzedaje baz użytkowników.

11. Google, Discord, Roblox i ER:LC

11.1. Google

Google uwierzytelnia użytkownika i przekazuje mChoroszczRP dane profilu objęte konfiguracją logowania: identyfikator, e-mail, imię, nazwisko i zdjęcie. Google może równocześnie przetwarzać dane o logowaniu jako odrębny administrator zgodnie z własną polityką.

11.2. Discord

Jeżeli administrator skonfiguruje webhook, treść wybranych zdarzeń, zgłoszeń lub logów może zostać wysłana do kanału Discord. Nie należy przysyłać przez webhook haseł, tokenów Google, tajnych kluczy, pełnych adresów IP ani danych zbędnych.

11.3. Roblox i ER:LC

Nick Roblox i informacje o statusie gracza mogą być porównywane z listą graczy online. Polecenia wysłane do ER:LC mogą zawierać nick i treść komunikatu. Integracja nie powinna przekazywać prawdziwego imienia i nazwiska z Google, chyba że jest to wyraźnie konieczne i opisane.

11.4. Hosting

Dostawca serwera może mieć techniczny dostęp do plików, bazy, logów i kopii zapasowych w zakresie niezbędnym do utrzymania infrastruktury. Administrator powinien wybrać dostawcę zapewniającego odpowiednie środki bezpieczeństwa.

12. Transfer danych poza Europejski Obszar Gospodarczy

Niektórzy dostawcy, w szczególności Google, Discord lub Roblox, mogą przetwarzać dane również poza Europejskim Obszarem Gospodarczym. Szczegóły zależą od organizacji infrastruktury danego dostawcy.

W przypadku transferu poza EOG administrator lub dostawca powinien stosować mechanizm przewidziany w rozdziale V RODO, np. decyzję stwierdzającą odpowiedni stopień ochrony, standardowe klauzule umowne lub inne właściwe zabezpieczenia.

Użytkownik może poprosić administratora o informację o stosowanych zabezpieczeniach. Jeżeli mChoroszczRP korzysta wyłącznie z hostingu na terenie EOG, nie wyklucza to transferów realizowanych niezależnie przez Google albo inne platformy.

13. Okres przechowywania danych

Dane konta i postaci są przechowywane przez okres aktywności konta oraz do czasu jego usunięcia albo zakończenia usługi. Po usunięciu część danych może pozostać przez okres potrzebny do wykonania kopii zapasowych, zabezpieczenia roszczeń i wyjaśnienia nadużyć.

Dane z Google są przechowywane tak długo, jak konto pozostaje powiązane z mChoroszczRP. Aktualne zdjęcie profilowe lub nazwa mogą zostać odświeżone przy kolejnym logowaniu, zależnie od implementacji.

Logi techniczne i bezpieczeństwa są przechowywane przez okres uzasadniony ryzykiem, zwykle nie dłużej niż jest to potrzebne do analizy incydentów, ochrony przed powtarzającymi się nadużyciami oraz dochodzenia lub obrony roszczeń.

Treść reklamacji i korespondencji może być przechowywana do zakończenia sprawy, a następnie przez okres przedawnienia potencjalnych roszczeń. Dane wymagane przepisem prawa są przechowywane przez okres wskazany w tym przepisie.

Kopie zapasowe mogą być nadpisywane cyklicznie. Natychmiastowe usunięcie pojedynczego rekordu z każdej kopii może być technicznie niemożliwe; dane nie powinny być jednak przywracane do aktywnego użycia poza sytuacją awaryjną.

14. Bezpieczeństwo danych

Administrator stosuje środki organizacyjne i techniczne odpowiednie do ryzyka, w szczególności logowanie Google, kontrolę uprawnień, sesje, ochronę CSRF, filtrowanie danych wyjściowych, szyfrowane połączenie HTTPS, ograniczenie dostępu do bazy i logi administracyjne.

Hasło do konta Google nie jest przekazywane mChoroszczRP. Proces uwierzytelnienia odbywa się po stronie Google, a serwer powinien weryfikować autentyczność otrzymanego tokenu lub kodu.

Dostęp do kont ROOT i administracyjnych powinien być szczególnie chroniony. Zaleca się wieloskładnikowe logowanie Google, ograniczenie liczby administratorów, regularne przeglądy uprawnień oraz nieudostępnianie kluczy API i webhooków.

Żaden system nie zapewnia absolutnego bezpieczeństwa. Użytkownik powinien zgłaszać podejrzane logowanie, nieudane próby migracji, nietypowe operacje i ujawnienie danych na kontakt@kubusekmeow.pl.

15. Prawa użytkownika

Wniosek można wysłać na kontakt@kubusekmeow.pl albo zgłosić telefonicznie pod numerem 71 707 23 91. Dla bezpieczeństwa administrator może poprosić o potwierdzenie konta Google lub inne proporcjonalne potwierdzenie tożsamości.

Odpowiedź powinna zostać udzielona bez zbędnej zwłoki, zasadniczo w terminie wynikającym z RODO. Termin może zostać przedłużony w przypadkach przewidzianych prawem, o czym osoba zostanie poinformowana.

- prawo dostępu do danych i otrzymania ich kopii;
- prawo sprostowania nieprawidłowych danych;
- prawo usunięcia danych, gdy zachodzą przesłanki prawne;
- prawo ograniczenia przetwarzania;
- prawo przenoszenia danych przetwarzanych automatycznie na podstawie zgody lub umowy;
- prawo sprzeciwu wobec przetwarzania opartego na prawnie uzasadnionym interesie;
- prawo wycofania zgody w dowolnym momencie, jeżeli zgoda jest podstawą;
- prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

16. Usunięcie konta i cofnięcie dostępu Google

Użytkownik może zażądać usunięcia konta przez kontakt z administracją. Usunięcie konta powoduje utratę dostępu do postaci, dokumentów RP, pojazdów, salda i historii rozgrywki, z zastrzeżeniem danych przechowywanych na podstawie prawa lub uzasadnionego interesu.

Cofnięcie dostępu mChoroszczRP w ustawieniach konta Google zatrzymuje przyszłe logowania, lecz nie usuwa automatycznie danych już zapisanych w bazie mChoroszczRP. Aby usunąć dane, należy dodatkowo wysłać żądanie do administratora.

Jeżeli konto jest objęte blokadą lub postępowaniem wyjaśniającym, administrator może zachować ograniczony zestaw danych potrzebny do ochrony innych użytkowników i roszczeń, mimo usunięcia aktywnego profilu.

Usunięcie konta z systemu nie powoduje usunięcia konta Google, Roblox ani Discord.

17. Dane dzieci i osób niepełnoletnich

mChoroszczRP może być używany przez osoby niepełnoletnie. Administrator powinien stosować szczególną ostrożność, prosty język, minimalizację danych i ograniczenie widoczności profilu.

Osoba niepełnoletnia nie powinna wpisywać prawdziwego adresu, szkoły, klasy, numeru telefonu, lokalizacji, prywatnych zdjęć ani danych pozwalających na kontakt poza kontrolowanymi kanałami.

Jeżeli przetwarzanie odbywa się na podstawie zgody w związku z usługą społeczeństwa informacyjnego oferowaną bezpośrednio dziecku, zastosowanie mają warunki z art. 8 RODO. Gdy wymaga tego prawo, zgodę wyraża lub zatwierdza rodzic albo opiekun.

Rodzic lub opiekun może skontaktować się z administratorem, jeżeli uważa, że dziecko utworzyło konto bez odpowiedniego uprawnienia albo ujawniło nadmierne dane. Administrator może poprosić o rozsądne potwierdzenie relacji i tożsamości.

18. Profilowanie i decyzje automatyczne

System może stosować proste automatyczne reguły, np. blokadę po wielu nieudanych próbach, ograniczenie konta wymagającego migracji Google, kontrolę uprawnień, zależności zakupów, cooldown oraz automatyczne odjęcie mandatu RP od salda.

Takie reguły służą wykonaniu usługi i bezpieczeństwu. Co do zasady nie wywołują skutków prawnych w świecie rzeczywistym ani nie wpływają na sytuację użytkownika poza fikcyjną rozgrywką.

Jeżeli automatyczna decyzja istotnie ogranicza konto, użytkownik może poprosić o ręczne sprawdzenie sprawy przez administrację. mChoroszczRP nie wykorzystuje danych Google do reklamowego profilowania ani ustalania zdolności kredytowej.

19. Naruszenia ochrony danych

W przypadku podejrzenia naruszenia ochrony danych administrator powinien ocenić jego charakter, zakres, kategorie danych, liczbę osób, możliwe skutki oraz zastosowane zabezpieczenia.

Jeżeli naruszenie może powodować ryzyko dla praw lub wolności osób, administrator podejmuje działania wymagane przez RODO, w tym w razie potrzeby zgłoszenie organowi nadzorcemu. Przy wysokim ryzyku osoby mogą zostać poinformowane bezpośrednio.

Użytkownik, który zauważy ujawnienie bazy, tokenu, zdjęć profili, adresów e-mail, logów lub nieuprawniony dostęp, powinien nie publikować danych dalej i niezwłocznie powiadomić administratora telefonicznie lub mailowo.

20. Zmiany polityki

Polityka może być aktualizowana w związku ze zmianą funkcji, dostawców, zakresu danych Google, okresów przechowywania, prawa lub środków bezpieczeństwa.

O istotnej zmianie użytkownik zostanie poinformowany w panelu, na stronie logowania lub innym odpowiednim kanałem. Jeżeli zmiana dotyczy celu wymagającego zgody, administrator powinien uzyskać nową zgodę przed rozpoczęciem takiego przetwarzania.

Data ostatniej aktualizacji i numer wersji powinny być widoczne na początku dokumentu. Archiwalne wersje mogą być przechowywane w celu wykazania, jakie informacje obowiązywały w danym okresie.

21. Skrócona tabela przetwarzania

Poniższa tabela podsumowuje najważniejsze operacje. Powinna zostać zaktualizowana, jeżeli rzeczywiste działanie systemu różni się od opisu.

Dane	Cel	Podstawa	Odbiorcy	Okres
Google ID, e-mail, imię, nazwisko, zdjęcie	Logowanie i profil OOC	art. 6 ust. 1 lit. b RODO	Google, hosting, administratorzy	Do usunięcia lub odłączenia konta, z zastrzeżeniem logów
Nick OOC i dane postaci IC	Konto i rozgrywka	art. 6 ust. 1 lit. b RODO	Upoważnieni użytkownicy i administratorzy	Przez czas prowadzenia konta
Nick Roblox i Discord	Integracje i kontakt	art. 6 ust. 1 lit. b/f RODO	Roblox/ER:LC, Discord, administratorzy	Do zmiany, usunięcia lub końca konta
IP, sesja, logi	Bezpieczeństwo i rozliczalność	art. 6 ust. 1 lit. f RODO	Hosting, administratorzy, organy gdy wymagane	Przez okres potrzebny do bezpieczeństwa i roszczeń
Zgłoszenia i wpisy Policji RP	Prowadzenie gry i moderacja	art. 6 ust. 1 lit. b/f RODO	Funkcjonariusze RP, dyżurni, administratorzy	Do zamknięcia sprawy i przez okres historii RP

22. Podstawy prawne i informacje końcowe

Politykę opracowano z uwzględnieniem RODO, polskiej ustawy o ochronie danych osobowych, ustawy o świadczeniu usług drogą elektroniczną oraz przepisów dotyczących przechowywania informacji i dostępu do informacji w urzędzeniu końcowym.

RODO wymaga przekazania osobie m.in. informacji o administratorze, celach, podstawach prawnych, odbiorcach, okresie przechowywania, prawach oraz ewentualnych transferach. Dokument powinien odpowiadać faktycznemu działaniu systemu, a nie jedynie planowanym funkcjom.

Google w ramach OpenID Connect może przekazywać podstawowe informacje profilu, gdy aplikacja żąda zakresów openid, profile i email. Zakres profile może obejmować m.in. imię, nazwisko i zdjęcie, a zakres email - adres e-mail.

Data obowiązywania polityki: 11 lipca 2026 r.

Podstawowe akty i standardy

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO), w szczególności art. 5, 6, 8, 12-22, 28, 32-34 i 44-49.

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną - tekst jednolity: Dz.U. z 2024 r. poz. 1513.

Ustawa z dnia 12 lipca 2024 r. - Prawo komunikacji elektronicznej, Dz.U. z 2024 r. poz. 1221.