24 Domeny.pl

RODO

Jak uniknąć bólu głowy dostosowując stronę do nowych przepisów?

Najważniejsze informacje o RODO

Co to jest RODO?

RODO (Rozporządzenie o Ochronie Danych Osobowych, lub – w wersji angielskiej GDPR - General Data Protection Regulation) będzie obowiązywać od 25 maja 2018 roku. To akt prawny, na nowo regulujący zagadnienia ochrony i przetwarzania danych osobowych.

Każdy podmiot przetwarzający dane jest zobowiązany do wprowadzenia wszelkich właściwych i niezbędnych zmian organizacyjnych i technicznych w aplikacjach, a także na stronach internetowych, do tego dnia.

Co to jest przetwarzanie?

„Przetwarzanie" dotyczy zbierania, rejestrowania, organizowania, strukturyzowania, przechowywania, adaptacji lub modyfikacji danych, wyszukiwania, konsultowania, używania, ujawniania w drodze transmisji, rozpowszechniania lub udostępniania w każdy inny sposób, dostosowania lub łączenia, ograniczania, usuwania lub niszczenia danych osobowych", zgodnie z art. 4 ust. 2 rozporządzenia RODO.

Co to są dane osobowe?

Dane osobowe to dane umożliwiające identyfikację osoby fizycznej, której dane dotyczą, bez używania niewspółmiernych sił i środków. Oznacza to, że „Adam" nie jest daną osobową, bo istnieją tysiące osób w Polsce o tym imieniu i dysponując tylko imieniem musielibyśmy stosować niewspółmierne siły i środki, aby zidentyfikować konkretnego Adama, np. spotkać się z każdym z nich.

Natomiast połączenie imienia z nazwiskiem, nazwą firmy, albo adresem z całą pewnością powoduje, że dane stają się danymi osobowymi.

Nowe przepisy rozszerzają definicję pojęcia danych osobowych, tak by uwzględniała ona możliwości rozwoju technologicznego i pojawienie się nowych form identyfikacji (dane genetyczne/dane biometryczne/dane dotyczące zdrowia).

W zasadzie jednak mało która strona internetowa dziś działa w oparciu o dane biometryczne, w większości wypadków zatem te postanowienia nie będą Cię dotyczyć

25. maja 2018

WEJŚCIE W ŻYCIE RODO

Przed i po – wybrane zagadnienia

Główne zmiany

Najważniejsze informacje, które warto znać, będąc webmasterem. Nie są one wyjątkowo duże, jeśli Twój serwis jest przygotowany zgodnie z dotąd obowiązującymi przepisami o ochronie danych osobowych, to większość przygotowanej dokumentacji lub formuły zgody wymaga tylko niewielkich poprawek.

Wdrożenie nowych przepisów jest natomiast dobrą okazją do zrewidowania, czy stosujesz wszystkie wymagania.

UWAGA! W tym dokumencie omawiamy wybrane zagadnienia, związane z korzystaniem z usług hostingowych oraz prowadzeniem strony www – nie jest to w żadnym razie kompletny poradnik omawiający wszystkie zagadnienia, związane z RODO, które mogą dotyczyć Twojej firmy, takie jak przetwarzanie zbiorów poza firmą hostingową, przetwarzanie zbiorów papierowych, danych kadrowych, dokumentów organizacyjnych itp.

do 25. maja 2018	od 25. maja 2018
Przetwarzanie wymaga zgody	Przetwarzanie nadal wymaga zgody
Treść zgody nie musi być notowana	Treść zgody powinna być notowana obok faktu jej wyrażenia
Obowiązek informowania o tym, kto jest administratorem	Obowiązek informowania o tym, kto jest administratorem oraz **kontaktu** do Inspektora Ochrony Danych, jeśli został powołany
Zbiory muszą być rejestrowane w GIODO albo w rejestrze ABI.	Nie ma obowiązku zgłaszania do zewnętrznego, centralnego rejestru, ale musi istnieć rejestr wewnątrz organizacji
Arbitralne wymagania minimalne, np. dotyczące złożoności haseł	Zasada **szacowania ryzyka** – administrator sam decyduje o sile hasła i innych środkach bezpieczeństwa
Administrator Bezpieczeństwa Informacji	Inspektor Ochrony Danych
	Obwiązek informowania o naruszeniu danych
Prawo do sprawdzania, poprawiania, żądania zaprzestania przetwarzania swoich danych osobowych	Prawo do sprawdzania, poprawiania, **przenoszenia** oraz żądania zaprzestania przetwarzania swoich danych osobowych
Umowa powierzenia w klasycznej formie papierowej	Umowa powierzenia nie musi być w formie papierowej
	Obwiązek informowania o naruszeniu danych
	Obowiązek informowania o profilowaniu
	Znacznie większe kary administracyjne niż do tej pory (do 4% obrotu rocznego lub do 20 mln EUR w razie nieprawidłowości).

Istotne zasady przetwarzania danych

Jako Administrator danych powinieneś upewnić się, że twoje działania są przejrzyste, a cel przetwarzania danych jest zgodny z prawem. Oznacza to, każdorazową potrzebę udowodnienia zasadności powodów do przetwarzania danych osobowych obywateli Polski oraz UE. Zgodnie z zasadą rozliczalności RODO powinieneś móc w łatwy sposób opisać cały proces pozyskiwania danych osobowych, które chcesz przetwarzać. Formuła wyrażonej na przetwarzanie zgody powinna być zapisana wraz z danymi osobowymi.

Sami przetwarzamy dane jedynie w zakresie niezbędnym do realizacji celów, na które zgadza się nasz użytkownik i to samo rekomendujemy użytkownikom usług hostingowych. Jeśli zatem masz stronę www i formularz np. zapisania na newsletter, w którym jest pole na wpisanie np. kodu pocztowego, którego nigdy nie wykorzystujesz później w żaden sposób – to oznacza, że zbierasz dane osobowe, które są Ci niepotrzebne. Tego typu dane nie mogą zostać uznane za adekwatne do wysłania newslettera i powinieneś zaprzestać ich przetwarzania, chyba, że masz inny, uzasadniony cel ich przetwarzania.

Masz prawo do wprowadzania zmian w swoich danych osobowych przetwarzanych przez nas. Edycja danych jest możliwa poprzez Panel Klienta.

Jako Administrator danych musisz upewnić się, że wszystkie przetwarzane dane są aktualne. Dane osobowe, które są niedokładne lub nieaktualne, powinny zostać natychmiast usunięte lub zmienione. Udostępnij użytkownikom narzędzia do edycji swoich danych lub zadbaj o to, żeby w jasny i dostępny dla siebie sposób mogli poprawiać swoje dane osobowe.

Przechowujemy dane osobowe każdego użytkownika nie dłużej niż jest to konieczne do celów, dla których dane osobowe są przetwarzane. Jeśli w Twoim serwisie przetwarzasz dane osobowe, to Ty także, jako Administrator danych, musisz upewnić się, że nie przechowujesz danych osobowych swoich potencjalnych klientów dłużej niż jest to konieczne do celów, dla których są przetwarzane.

Co musi wiedzieć właściciel strony?

Muszę mieć nowe check-boxy?

W zakresie pozyskania zgody na przetwarzanie danych osobowych nie ma radykalnych zmian. Jeśli dobrze przygotowałeś check-boxy związane z pozyskiwaniem danych na gruncie obecnych przepisów – zmiany są stosunkowo niewielkie.

Do głównych zmian należy konieczność podania informacji o prawie do przenoszenia danych, okresie przechowywania, zamiarze ich przekazania do państw trzecich, etc. Należy także podać kontakt do inspektora ochrony danych (IOD), o ile takowy zostaje powołany. Należy także informować, że dane będą wykorzystywane do profilowania.

Treść zgody wraz z oznaczeniem czasu jej wyrażenia powinna być zapisana w rejestrze zgód – w powiązaniu z identyfikatorem osoby, której one dotyczą.

Podsumowując zatem: Należy dopasować treść check-boxów na stronie, ale nowe przepisy wcale nie oznaczają, że będzie ich więcej niż do tej pory. Na kolejnej stronie znajdziesz zakres wymaganych informacji, jakie masz obowiązek przekazywać.

Jak często mam zmieniać hasła?

Nowe przepisy operują pojęciem ryzyka. Im większe jest ryzyko, na które narażone są przetwarzane dane osobowe, tym większe obowiązki administratora w zakresie ochrony danych.

O ile na przykład poprzednie przepisy nakazywały stosowanie haseł min. 8 znakowych, o określonej złożoności, zmienianych raz na 30 dni, przy przetwarzaniu na poziomie wysokim w zasadzie we wszystkich sytuacjach przetwarzania danych osobowych w internecie, o tyle nowe przepisy kładą nacisk na stosowanie zabezpieczeń adekwatnie do chronionych danych i sposobu ich przetwarzania, pozostawiając administratorowi ocenę, czy powinno to być 30, czy może raczej 14 dni.

Naszym zdaniem w większości przypadków 30 dni to rozsądny interwał do zmiany haseł na stronach i w aplikacjach internetowych w większości zastosowań.

Zgłaszanie naruszeń

Nowe przepisy nakładają na administratorów danych poważny obowiązek zgłaszania naruszeń. W razie powzięcia przed administratora informacji o naruszeniu bezpieczeństwa danych ma on obowiązek poinformować osoby, których te dane dotyczą oraz organ nadzoru, a niedochowanie tego obowiązku może wiązać się z wysokimi karami.

Co musi wiedzieć właściciel strony?

Obowiązek informacyjny

Jeśli zbierasz dane osobowe na swojej stronie internetowej (choćby sam adres e-mail) to musisz dopełnić obowiązków informacyjnych względem osób, których dane dotyczą. Masz obowiązek przekazania im czytelnej informacji o następującym zakresie:

1. Kto jest administratorem danych (+dane kontaktowe)
2. Jeśli jest powołany Inspektor Ochrony Danych – jego dane kontaktowe.
3. Cel przetwarzania danych
4. Podstawa prawna przetwarzania danych
5. Zamiar przekazania danych innemu podmiotowi - jeśli taki zamiar występuje, czyli tzw. informacja o odbiorcach danych
6. Zamiar przekazania informacji do państwa trzeciego, lub organizacji międzynarodowej, jeśli występuje.
7. Jak długo dane będą przechowywane
8. Informację o prawie do:
    1. wglądu do danych
    2. zmiany danych lub ich usunięcia z bazy
    3. wycofania zgody na przetwarzanie, które musi być tak samo proste, jak jej wyrażenie
    4. przeniesienia danych
9. Informację o prawie wniesienia skargi do organu nadzorczego (aktualnie: GIODO).
10. Informacje o profilowaniu, jeśli mają one zastosowanie.

Co musi wiedzieć właściciel strony?

Projektowanie aplikacji

Nowe regulacje wskazują na konieczność uwzględniania zasad ochrony danych osobowych już w fazie projektowania nowych systemów i aplikacji. Warto zatem, tworząc nową aplikację lub stronę www, mieć na względzie mechanizmy wspierające ich ochronę.

Hosting a dane osobowe

Firma hostingowa jest administratorem danych osobowych zbiorów, które tworzy, jak np. zbiór klientów oraz osób kontaktowych klientów, zbiór potencjalnych klientów, zbiór osób zapisanych na newsletter itp.

Firma hostingowa jest procesorem danych w odniesieniu do wszelkich danych umieszczonych na serwerze przez jej klientów. Ponieważ firma hostingowa nie wie, którzy klienci umieścili na jej serwerach dane osobowe, jeśli tak się dzieje – konieczne jest zawarcie umowy powierzenia przetwarzania danych osobowych.

Umowa powierzenia

Umowa powierzenia na gruncie obowiązujących przepisów wymagała formy pisemnej (papierowej). Nowe przepisy nie przewidują obowiązku zachowania takiej formy, zatem będzie możliwość zawierania umowy w formie czysto elektronicznej, co znacznie skróci i uprości ten proces.

W grupie H88, na dzień przygotowania tego opracowania, nie przewidujemy żadnych opłat dodatkowych, związanych z zawieraniem tego rodzaju standardowej umowy elektronicznej. Wprowadzimy możliwość zawierania tego rodzaju umów poprzez panel klienta.

Audyt – czy go potrzebujesz?

Naszym zdaniem, jeśli chcesz poprawić swoje poczucie pewności w obliczu zbliżających się zmian prawnych – zlecenie specjalistycznego audytu w Twojej firmie może być celowe. Audyt taki powinien obejmować wszystkie obszary działalności, a nie tylko dane, które przetwarzasz w ramach powierzenia firmie hostingowej. Dlatego uważamy, że firma hostingowa nie jest w stanie skutecznie i efektywnie audytować tego obszaru w całości.

Uważamy, że w obszarze Twojego styku z firmą hostingową najważniejszą sprawą jest zawarcie umowy powierzenia i uwzględnienie w Twojej stronie www wszystkich wytycznych oraz dobrych praktyk, które wskazujemy w tym dokumencie.

Usługa zawarcia standardowej umowy powierzenia w oparciu o RODO – forma elektroniczna

0,-zł

Dobre praktyki

To może Cię zainteresować

Szyfrowanie – tj. zapisanie w bazie informacji w postaci zaszyfrowanej tak, że nie jest możliwe jej odczytanie przez osoby postronne w razie wykradzenia bazy danych.

Pseudonimizacja – Usunięcie danych osobowych i zastąpienie ich znacznikiem – identyfikatorem uniemożliwiającym identyfikacje konkretnej osoby fizycznej nikomu, kto nie posiada „rozwiązania" identyfikatora na dane konkretnej osoby.

Anonimizacja – całkowite i nieodwracalne usunięcie ze zbioru informacji umożliwiających identyfikację konkretnej osoby fizycznej przez kogokolwiek.

Hashowanie – zapisanie wyniku działania funkcji skrótu, tworzącej unikalny i praktycznie nieodwracalny skrót o zadanej długości z dowolnego ciągu bitów. W ten sposób możesz zapisać np. adres mailowy osoby, która zgłasza sprzeciw wobec przetwarzania – nie można tego procesu odwrócić i dowiedzieć się, jaki do był adres, ale można dowieść, że dla konkretnego adresu sprzeciw wyrażono.

Projektowanie	Hosting	Implementacja
Uwzględnienie wszystkich aktualnych wymagań z naciskiem na zgody oraz środki ochrony	Umowa powierzenia z firmą hostingową	Ochrona certyfikatem SSL
Szacowanie ryzyka		Dwuczynnikowa autentykacja
Dokumentacja		Zabezpieczenie strony logowania dla wybranych IP
Odpowiednie zgody		Zabezpieczenia w .htaccess
Double opt-in		Szkolenie pracowników
Ograniczenie czasu przechowywania danych		

Cookies – a co z nimi?

Brak jednoznacznych wytycznych, ale...

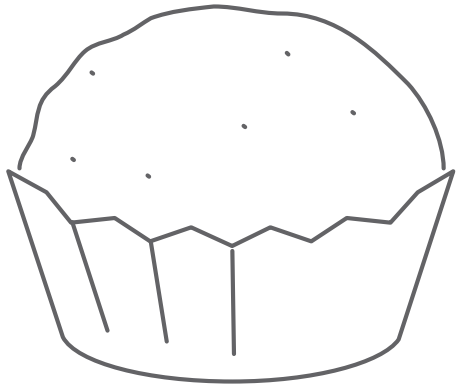
Aktualnie nie ma jednoznacznych wytycznych, dot. stosowania ciastek w kontekście RODO. Same pliki cookies zazwyczaj nie zawierają danych osobowych, ale mogą być wykorzystywane do profilowania, tj, określania profilu użytkownika na podstawie jego zachowania na stronie, a ponadto mogą być w niektórych wypadkach połączone z danymi wprost identyfikującymi określoną osobę fizyczną, np. kiedy ciastko określające użytkownika zostanie powiązane z danymi konkretnej osoby podczas składania zamówienia.

Teoretycznie istnieje możliwość zapisania danych osobowych wprost w pliku cookie – np. imienia i nazwiska. Mimo, że jest to technicznie wykonalne, to nie zalecamy takiego rozwiązania, ponieważ tworzone w ten sposób zbiory danych osobowych będą zapisywanie w środowisku, nad którym, jako administrator danych, masz bardzo ograniczoną kontrolę, albo też nie masz jej wcale - użytkownik może bowiem w dowolnej chwili zawartość ciastka zmienić albo całkowicie je usunąć.

... wciąż obowiązuje Prawo Telekomunikacyjne

RODO nie zmienia niczego jeśli o obowiązki wynikające z Prawa Telekomunikacyjnego. Art. 173 mówi wyraźnie o konieczności uzyskania zgody na przechowywanie cookies od właścicieli przeglądarki / urządzenia końcowego.

Zgoda ta może być wyrażona odpowiednimi ustawieniami przeglądarki, ale użytkownik musi mieć możliwość zapoznania się z tym, do czego są wykorzystywane pliki cookies – standardowo tego rodzaju informacje umieszczane są w polityce prywatności.



Certyfikat SSL a dane osobowe

Co to jest?

Certyfikat SSL służy potwierdzeniu właściciela danej strony oraz szyfrowaniu komunikacji między przeglądarką internetową użytkownika a serwerem.

Wszystkie obecne na rynku certyfikaty posiadają zbliżone właściwości jeśli chodzi o szyfrowanie, różnią się natomiast innymi cechami, takimi jak wiarygodność albo liczba obsługiwanych domen / subdomen.

Czy muszę to mieć?

Przepisy mówią o stosowaniu szyfrowania jako środka ochrony danych osobowych, nie wymieniając jednak wprost certyfikatu SSL w Rozporządzeniu.

Jest to jednak najłatwiejszy I najtańszy sposób na zapewnienie zaszyfrowanej transmisji danych, a co za tym idzie – poufności danych osobowych, które pozyskujesz od użytkowników Twojej strony www.

Jakie inne metody warto rozważyć?

Dobrze mieć świadomość, że stosowanie certyfikatu SSL stanowi środek ochrony kryptograficznej w warstwie transmisji danych do serwera, ale nie zabezpiecza on danych znajdujących się po prostu na serwerze, w samej bazie.

Jest on – w naszej ocenie – koniecznym środkiem ochronnym w zasadzie w każdym systemie, gdzie dochodzi do przetwarzania danych. Szacując ryzyko w Twoim wypadku - musisz sam ocenić, czy należałoby zastosować dodatkowe, kryptograficzne środki ochronne. Należą do nich, np..: szyfrowanie danych w bazie albo szyfrowanie danych w warstwie PHP, zanim zostaną przesłane do bazy danych.

W naszej firmie możesz korzystać z funkcji szyfrujących zarówno w samej bazie, jak i w PHP. Nie wiąże się to z dodatkowymi opłatami ale chcąc wykorzystać te możliwości musisz przystosować swoją stronę/aplikację.

Żądanie zaprzestania przetwarzania a backup

Jak realizować do dobrze?

Polecamy Ci zapisywanie żądania zaprzestania danych z wykorzystaniem funkcji skrótu, czyli popularnego hasha, np. funkcji sha1(), wykonanej na danych osobowych.

W ten sposób w Twojej bazie nie będzie danych osobowych ani danych, które możliwiają odszyfrowanie danych osobowych. Hashowanie jest operacją jednokierunkową, nie pozwala na „odszyfrowanie" danych tak, jak w wypadku szyfrowania.

Hash jednak zawsze daje ten sam wynik, jeśli jest wykonany na tych samych danych, co oznacza, że jeśli chcesz sprawdzić, czy dana osoba wyraziła sprzeciw – możesz to zrobić nie mając jej danych, a jedynie hash. Wystarczy obliczyć hash z adresu mailowego i sprawdzić, czy posiadasz taki sam hash w bazie sprzeciwów – jeśli tak, to dany adres nie może być przetwarzany.

Backup danych

Prawo do bycia zapomnianym nie stoi nad obowiązkiem ochrony integralności zbioru danych. Masz prawo i powinieneś wykonywać backupy swoich zbiorów.

Jeśli ktoś zgłosi chęć skorzystania z prawa do bycia zapomnianym, naturalnie powinieneś go wykreślić z bazy oraz zanotować sprzeciw wobec dalszego przetwarzania jego danych, ale nie musisz automatycznie usuwać wszystkich backupów, w których te dane się znajdują.

Przy okazji... dobrze wiedzieć, jak długo firma hostingowa przechowuje backupy Twoich danych, które jej powierzysz. W naszym wypadku ten czas wynosi do

28 dni pliki www

7 dni bazy danych

Przykładowa checklista dla webmastera

- ☐ Uzyskuję zgody od osób, których dane dotyczą
- ☐ Informuję rzetelnie o celu przetwarzania danych
- ☐ Informuję o moich danych rejestrowych
- ☐ Informuję o moich danych kontaktowych
- ☐ Informuję o danych kontaktowych IOD o ile jest powołany
- ☐ Informuję o zakresie czasowym przetwarzania danych
- ☐ Informuję o podstawie prawnej przetwarzania
- ☐ Informuję o zamiarze profilowania lub skutkach działania automatycznych systemów podejmujących decyzję, pracujących na bazie podanych danych osobowych.
- ☐ Informuję o zamiarze przekazania danych innymi podmiotom
- ☐ Informuję o zamiarze przekazania danych do państwa trzeciego lub organizacji międzynarodowej
- ☐ Informuję o prawie do wglądu, poprawiania, ograniczenia przetwarzania, wycofania zgody na i przeniesienia danych
- ☐ Informuję o prawie do wniesienia skargi do organu nadzoru
- ☐ Stosuję metodę double opt-in w zapisie na newsletter

- ☐ Zawarłem umowę powierzenia z firmą hostingową
- ☐ Stosuję certyfikat SSL
- ☐ Stosuję szyfrowanie w warstwie PHP
- ☐ Stosuję szyfrowanie w warstwie MySql
- ☐ Stosuję hashownie danych co do których zgłoszono sprzeciw, prowadzę rejestr sprzeciwów.
- ☐ Daję użytkownikom możliwość poprawiania danych
- ☐ Daję osobie, której dane dotyczą, możliwość uzyskania informacji, jakiego rodzaju dane przetwarzam
- ☐ Automatycznie usuwam dane po okresie ich przydatności
- ☐ Upewniłem się, co do tego, czy nie zbieram zbyt dużego zakresu danych – wykraczając poza zasadę adekwatności
- ☐ Zapewniłem regularny backup danych osobowych
- ☐ Stosuję anonimizację danych tam, gdzie jest to uzasadnione biznesowo
- ☐ Stosuję ochronę ekranu logowania np. do określonego adresu IP, albo ograniczam próby logowania z danego adresu. Aktywnie korzystam z możliwości dyrektyw .htaccess w celu podniesienia poziomu bezpieczeństwa strony/aplikacji

UWAGA! Niniejsza lista ma na celu ułatwienie przygotowania Twojej strony www lub aplikacji. Nie jest wyczerpująca dla procesu przygotowania całego przedsiębiorstwa do RODO, ponieważ jest to proces wykraczający poza stronę www.

Moje dane jako klienta

Zakres danych

Przetwarzamy dane Klientów, korzystających z usług hostingowych, które obejmują następujące informacje:

- Imię i nazwisko
- Adres email
- PESEL
- Adres do korespondencji papierowej
- Adres siedziby
- Numery telefonów

Aktualność

Aktualność Twoich danych możesz w każdej chwili sprawdzić poprzez panel klienta w każdej naszej marce hostingowej.

Masz także prawo i możliwość zmiany swoich danych osobowych w dowolnym momencie, to również możesz zrealizować poprzez panel klienta.

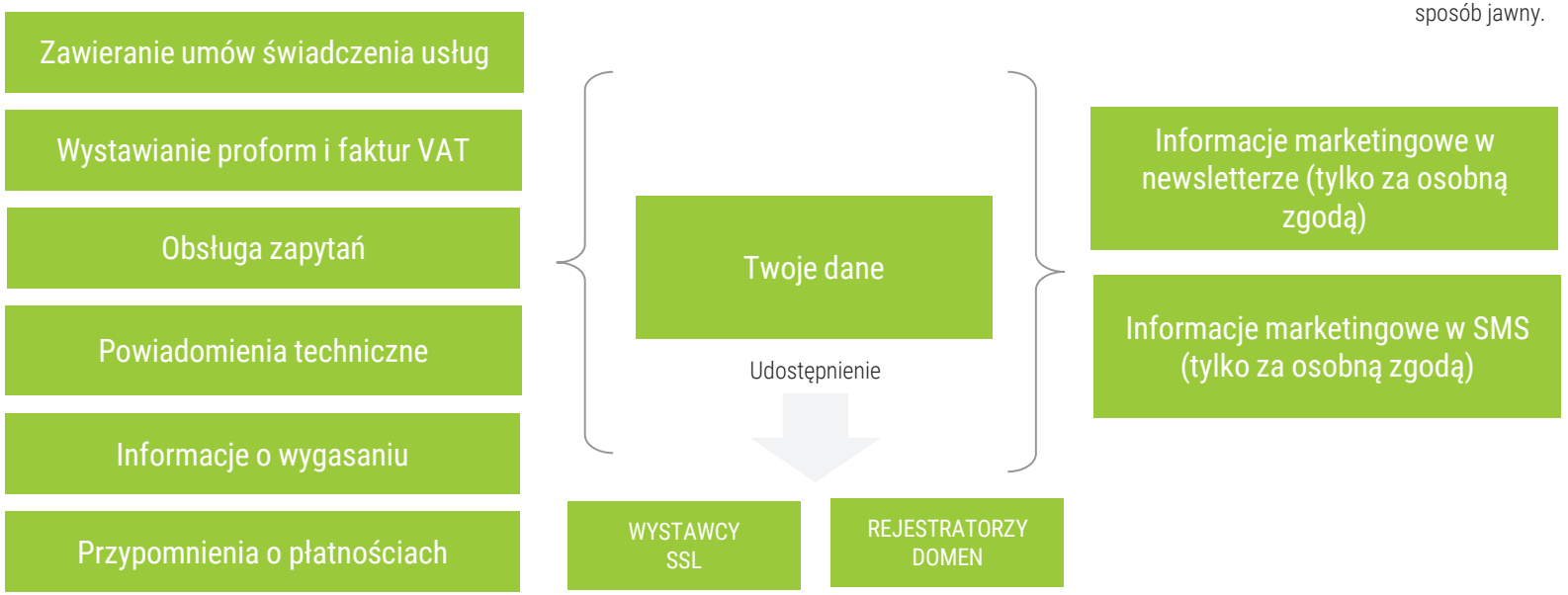
Cel przetwarzania

Twoje dane są przetwarzane w celu świadczenia usług z naszej oferty. Oznacza to przede wszystkim rejestrację domen, świadczenie usługi hostingu www, VPS, serwerów dedykowanych, usług sem/seo oraz innych usług o zbliżonym charakterze. Jeśli wyrażasz na to zgodę – możemy wysyłać Ci także informacje handlowe przy pomocy maili oraz SMS'ów.

Udostępnienie

Twoje dane są udostępniane podmiotom rejestrującym domeny (rejestratorom), jeśli korzystasz z usługi rejestracji i utrzymania domen. W największym stopniu dotyczy to NASK – Naukowej i Akademickiej Sieci Komputerowej. Dane są także udostępniane wystawcom certyfikatów SSL.

W wypadku innych usług nie udostępniamy Twoich danych osobowych chyba, że wyrazisz na to zgodę w sposób jawny.



Moje dane jako klienta

Logowanie

Twoje dane są przechowywane w systemach chroniących je na wypadek zarówno przypadkowego zniszczenia jak i nieupoważnionego dostępu.

Dane są przetwarzane w systemie rozproszonym, w architekturze klient-serwer. Logowanie do systemów zawierających Twoje dane jest możliwe wyłącznie dla upoważnionych pracowników po podaniu loginu oraz odpowiednio złożonego hasła. Hasła podlegają okresowym zmianom.

Wszelkie strony logowania do systemów przetwarzających Twoje dane osobowe są chronione certyfikatami SSL, a w większości wypadków – nałożone są dodatkowe ograniczenia dotyczące adresów IP, z których możliwe jest zalogowanie do takich systemów.

Centra danych

Wszystkie centra danych, z których korzystamy, to profesjonalnie przygotowane obiekty. W każdym z nich znajdują się środki ochrony przed niepowołanym dostępem osób nieuprawnionych, w tym:

- Systemy antywłamaniowe
- Bariery fizyczne i optyczne
- Monitoring
- Systemy kontroli dostępu
- Brak możliwości przebywania osób trzecich

Każde centrum danych zabezpieczone jest przed skutkami przerw w zasilaniu poprzez stosowanie min. dwóch niezależnych źródeł zasilania, w tym jednego opartego o agregaty prądotwórcze i systemy podtrzymania napięcia UPS.

W obiektach są stosowane mechanizmy ochrony przeciwpożarowej przystosowane do gaszenia urządzeń pod napięciem.

Serwery

Dane są zapisywane na dyskach twardych połączonych w macierze dyskowe. Stosowane są mechanizmy RAID 10, zapewniające ochronę danych w wypadku uszkodzenia jednego lub – w niektórych wypadkach – dwóch dysków twardych jednocześnie, bez utraty integralności danych.

Drugą linię ochrony stanowi backup, czyli cykliczne wykonywanie kopii danych na niezależnym urządzeniu, umożliwiającego przywrócenie danych nawet w razie całkowitej awarii głównego serwera.

Stosowane są redundantne zasilacze i karty zdalnego zarządzania.

Sieć

Stosowane są mechanizmy redundancji kluczowych elementów infrastruktury sieciowej oraz – częściowo - ochrony przed atakami typu DDoS, do poziomu 10 Gbps.

Organizacja

Stosujemy przewidziane przepisami rozwiązania organizacyjne w zakresie ochrony danych. Aktualnie w naszej firmie funkcjonuje Administrator Bezpieczeństwa Informacji, który zostanie zastąpiony Inspektorem Ochrony Danych.

Prowadzone są rejestry zbiorów danych oraz czynności przetwarzania.

Dbamy o dystrybucję wiedzy o ochronie danych osobowych wśród pracowników, poprzez prowadzenie wewnętrznych szkoleń.

Nasze działania w zakresie ochrony danych, których jesteśmy administratorem, podlegają procesom audytowania.

Moje dane powierzone (umowa powierzenia)

Logowanie

W tym wypadku to Ty decydujesz o środkach ochronnych w zakresie logowania do systemów umożliwiających przetwarzanie danych osobowych.

Centra danych i sieci

Stosowane są takie same mechanizmy jak w opisie danych, których jesteśmy administratorem. Stosowane są mechanizmy redundancji kluczowych elementów infrastruktury sieciowej oraz – częściowo - ochrony przed atakami typu DDoS, do poziomu 10 Gbps.

Umowę powierzenia zawierasz elektronicznie w swoim Panelu Klienta.

Serwery

Zakres stosowanych zabezpieczeń w znacznym stopniu zależy od rodzaju usługi.

Hosting współdzielony	Serwery VPS	Serwery dedykowane
Macierz RAID 1, 10 oraz 6 zależnie od usługi	Macierz RAID 10 oraz 6, zależnie od usługi	Macierz RAID 1,6,10 zależnie od wybranej konfiguracji)
Podwójne zasilacze	Podwójne zasilacze	Podwójne zasilacze
Redundantne chłodzenie	Redundantne chłodzenie	Redundantne chłodzenie
Zdalne zarządzanie pełne	Zdalne zarządzanie pełne	Zdalne zarządzanie ograniczone
Backup – zgodnie z informacją na stronie www	Backup – zgodnie z informacją na stronie www	Backup we własnym zakresie
Dostęp ROOT po stronie firmy hostingowej	Dostęp ROOT po stronie klienta, chyba, że wybrano usługę zarządzaną	Dostęp ROOT po stronie klienta, chyba, że wybrano usługę zarządzaną

Dziękujemy

Jeśli uważasz, że prezentacja była interesująca, podziel się nią śmiało ze znajomymi, wrzuć do mediów społecznościowych. Będzie nam miło.

Jeśli chcesz wiedzieć więcej albo zawrzeć umowę powierzenia:

Zapraszamy do kontaktu z naszym
Biurem Obsługi Klienta

https://www.a24.domeny.pl/