

# Środki ochrony danych osobowych stosowane w dhosting.pl Sp. z o.o.

## Proces przetwarzania danych osobowych w dhosting.pl Sp. z o.o. oparty jest na przepisach prawa, w szczególności:

1. Ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (zwanej dalej ustawą)
2. Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (zwanym dalej rozporządzeniem)
3. Innych przepisów szczególnych

Zgodnie z obowiązującymi przepisami prawa dotyczącymi ochrony danych osobowych dhosting.pl stosuje zabezpieczenia fizyczne i organizacyjne, środki ochrony w ramach narzędzi programowych oraz środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej zgodnie z art. 36-39 ustawy.

W trosce o zapewnienie prawidłowości przetwarzanych danych osobowych we wszystkich procesach biznesowych został wyznaczony w dhosting.pl Administrator Bezpieczeństwa Informacji zgodnie z art. 36 ust. 3. Funkcję tę pełni specjalistyczna firma posiadająca duże doświadczenie w zakresie zapewnienia wysokich standardów bezpieczeństwa.

Zastosowane środki ochrony w pełni gwarantują zachowanie poufności, integralności oraz rozliczalności przetwarzanych danych.

## Bezpieczeństwo fizyczne budynku i pomieszczeń

1. Budynek, w którym zlokalizowana jest serwerownia nadzorowany jest przez całą dobę przez służbę ochrony firmy ATM S.A.
2. W budynku zastosowany jest system monitoringu z użyciem kamer przemysłowych.
3. Dostęp do pomieszczeń objęty jest systemem kontroli poprzez wykorzystanie czytników kart.

4. Pomieszczenia zabezpieczone są drzwiami o podwyższonej odporności ogniowej.
5. Serwerownia ulokowana jest w ATM S.A. przy ul. Grochowskiej 21a na 2 kondygnacji, co uniemożliwia włamanie przy użyciu okien.
6. Pomieszczenia wyposażone są w system przeciwpożarowy.
7. Pomieszczenia serwerowni spełniają dodatkowo zalecenia klasy Tier-3 według normy ANSI TIA-942.

## Zabezpieczenia organizacyjne

1. Wszystkie zatrudnione osoby, które w ramach wykonywania swoich obowiązków służbowych mają dostęp do danych osobowych, posiadają pisemne, imienne upoważnienia, do których posiadania zobowiązuje art. 37 ustawy.
2. Wszystkie zatrudnione osoby posiadają pisemne, imienne upoważnienia, do których posiadania zobowiązuje art. 37 ustawy.
3. Wszystkie zatrudnione w dhosting.pl osoby, które w ramach wykonywania swoich obowiązków służbowych mają dostęp do danych osobowych, zostały przeszkolone z zakresu ochrony danych osobowych oraz zgodnie z art. 39 ust. 2 ustawy zostały zobowiązane do zachowania tych danych oraz sposobów ich zabezpieczania w tajemnicy.
4. Nośniki, zawierające dane osobowe przechowywane są w miejscach uniemożliwiających dostęp do nich osobom nieupoważnionym.
5. Zostały opracowane oraz wdrożone procedury wykonywania kopii zapasowych oraz dostępu do tych kopii.
6. Dostęp do kopii zapasowych posiadają wyłącznie osoby upoważnione.
7. Wdrożone zostały procedury organizacyjne dotyczące kontroli dostępu do systemów teleinformatycznych.

## Zabezpieczenia sprzętowe oraz środki ochrony narzędzi programowych

1. Dostęp do systemów teleinformatycznych posiadają jedynie uprawnieni użytkownicy.

2. Nadawanie uprawnień oraz stosowane metody uwierzytelniania się użytkowników są zgodne z wymaganiami rozporządzenia.
3. Zastosowane są urządzenia chroniące system informatyczny przed skutkami awarii zasilania.
4. Stosowane są środki kryptograficznej ochrony danych przekazywanych drogą teletransmisji.
5. W celu zabezpieczenia danych przed szkodliwym oprogramowaniem stosowany jest program antywirusowy oraz przed nieuprawnionym dostępem z sieci - system firewall.
6. Dane są przetwarzane wyłącznie w macierzach dyskowych RAID np. 1, 5, 10 zabezpieczających przed skutkami awarii pamięci dyskowej.
7. W przypadku konieczności wymiany uszkodzonego dysku, dane z napędu są kasowane przed przekazaniem dysku do naprawy przy pomocy oprogramowania służącego do zamazywania danych na dysku. Jeżeli dysk zawierający dane osobowe nie nadawałby się do naprawy, jest on, po logicznym usunięciu danych, niszczone fizycznie.