

W CD PROJEKT zwracamy szczególną uwagę na bezpieczeństwo informacji, które udostępniamy. Z tego powodu rekomendujemy, aby podmioty zewnętrzne z którymi współpracujemy, spełniały określone wymagania bezpieczeństwa.

Wyszczególniliśmy trzy poziomy wymagań bezpieczeństwa w zależności od krytyczności danych, które powierzamy.

Dla każdego z poziomów wrażliwości danych nasi kontrahenci powinni spełniać określone wymagania bezpieczeństwa z zakresu procedur, bezpieczeństwa fizycznego, zarządzania incydentami, zarządzania ciągłością działania, bezpieczeństwa danych, bezpieczeństwa infrastruktury oraz zarządzania dostępem i tożsamością.

Wymagania bezpieczeństwa dla średniego poziomu wrażliwości danych CDPR

1. Procedury

- 1.1. Kontrahent powinien posiadać i stosować zasady zarządzania urządzeniami mobilnymi oraz stosowne środki bezpieczeństwa obejmujące urządzenia mobilne używane do przetwarzania danych CDPR.
- 1.2. Wszyscy pracownicy Kontrahenta oraz, w stosownych przypadkach, jego kontrahenci powinni być przeszkoleni z obszaru świadomości bezpieczeństwa oraz być regularnie informowani o zasadach i procedurach organizacyjnych, stosownie do pełnionych przez nich funkcji.
- 1.3. Kontrahent powinien posiadać i stosować zasady zarządzania nośnikami wymiennymi.
- 1.4. Przed rozpoczęciem przez Kontrahenta współpracy z podmiotem zewnętrznym obejmującej udostępnienie temu podmiotowi jakichkolwiek danych CDPR, Kontrahent upewni się, że dostęp tego podmiotu został zatwierdzony przez CDPR.

2. Bezpieczeństwo fizyczne

- 2.1. Kontrahent powinien stosować środki fizycznej kontroli dostępu (np. zamki z kluczem, kamery, czytniki kart, systemy alarmowe) wokół obszarów, w których przetwarzane są dane CDPR.
- 2.2. Wszystkie zasoby fizyczne, które służą do przetwarzania danych CDPR (np. zewnętrzne dyski twarde, materiały drukowane) powinny być przechowywane w bezpiecznej lokalizacji fizycznej.

- 2.3. Goście wchodzący do obszaru, w którym przetwarzane są dane CDPR, powinni być rejestrowani.
- 2.4. Gościom przebywającym w obszarze, w którym przetwarzane są dane CDPR, powinien stale towarzyszyć przedstawiciel Kontrahenta.

3. Zarządzanie incydentami

- 3.1. Kontrahent powinien wskazać osobę odpowiedzialną za kluczowe obszary bezpieczeństwa i udostępnić CDPR dane kontaktowe tej osoby.
- 3.2. Każdy incydent bezpieczeństwa mogący obejmować dane CDPR powinien być niezwłocznie zgłaszany na security@cdprojektred.com.

4. Bezpieczeństwo danych

- 4.1. Kontrahent powinien zidentyfikować zasoby informatyczne używane do przetwarzania danych CDPR oraz prowadzić ich spis. Wszystkie te zasoby informatyczne powinny mieć zdefiniowanych właścicieli odpowiedzialnych za ich bezpieczne i prawidłowe działanie.
- 4.2. Sprzęt i oprogramowanie służące do przetwarzania danych CDPR powinny być regularnie aktualizowane pod względem bezpieczeństwa. Kontrahent powinien na bieżąco monitorować dostępność aktualizacji bezpieczeństwa dla poszczególnych składników sprzętu i oprogramowania.
- 4.3. Tylko osoby, którym kontrahent zleca pracę z danymi CDPR mogą mieć dostęp do tych danych.
- 4.4. Każda osoba, której kontrahent zleca pracę z danymi CDPR, powinna mieć podpisaną ważną umowę o zachowaniu poufności z kontrahentem.
- 4.5. Kontrahent powinien mieć podpisaną z CDPR ważną umowę o zachowaniu poufności.
- 4.6. Kontrahent powinien posiadać wdrożone środki ochrony przed złośliwym oprogramowaniem (wykrywanie, zapobieganie, odzyskiwanie), w szczególności regularnie tworzyć kopie zapasowe danych na odrębnym nośniku.
- 4.7. Kontrahent powinien zapewnić stałą ochronę danych CDPR przez ich szyfrowanie w spoczynku i w czasie przesyłania.
- 4.8. Kontrahent powinien przysyłać dane CDPR w formie zaszyfrowanej lub przysyłać je przez kanał zapewniający szyfrowanie (np. VPN).

5. Bezpieczeństwo infrastruktury

- 5.1. Kontrahent powinien wdrożyć łączność sieciową opartą na najniższych uprawnieniach, zgodnie z regułą zero-trust, segmentację sieci (np. przez VLAN) lub fizyczną rozdzielność zasobów sieciowych.
- 5.2. Zdalny dostęp do sieci wewnętrznej kontrahenta, w której przetwarzane są dane CDPR, powinien być ograniczony i możliwy tylko za pośrednictwem połączenia VPN, które w ramach procesu logowania wymaga uwierzytelniania wieloskładnikowego.

6. Zarządzanie dostępem i tożsamością

- 6.1. Systemy informatyczne, w których przetwarza się dane CDPR, powinny być dostępne po zalogowaniu indywidualnym loginem i hasłem użytkownika.
- 6.2. Każdy użytkownik powinien mieć dostęp tylko do takich danych CDPR, których faktycznie potrzebuje (segmentacja zasobów oraz różnicowanie dostępu na zasadzie wiedzy koniecznej).
- 6.3. Kontrahent powinien nadawać, odbierać i modyfikować dostępy użytkowników na bieżąco, w miarę aktualnych potrzeb (zatrudnienie pracownika, odejście pracownika, zmiana roli lub zakresu pracy).