Załącznik nr 1 do umowy z dnia

# Wykaz sposobów zapewnienia zasad bezpieczeństwa danych osobowych i bezpieczeństwa przetwarzanych informacji

|  |  |  |
| --- | --- | --- |
| **Wymaganie** | **Tak / Nie / Nie dotyczy** | **Dowód lub szczegółowy opis spełnienia wymagania** |
| Czy Wykonawca (dalej podmiot przetwarzający) posiada opracowaną i zatwierdzoną politykę ochrony danych osobowych? Proszę o wskazanie nazwy ww. dokumentu wraz z datą zatwierdzenia oraz nadanym numerem wewnętrznym. |  |  |
| Czy podmiot przetwarzający prowadzi Rejestr Wszystkich Kategorii Przetwarzania? |  |  |
| Czy podmiot przetwarzający zapewnia, że nowo zatrudniony pracownik przed podjęciem czynności związanych z przetwarzaniem danych osobowych zostanie odpowiednio przeszkolony w tym zakresie i zapoznany z obowiązującymi przepisami prawa? |  |  |
| Czy podmiot przetwarzający dba o bieżące doskonalenie wiedzy swoich pracowników dzięki cyklicznym szkoleniom oraz innym działaniom mającym na celu uświadamianie pracowników w zakresie zagadnień dotyczących ochrony danych osobowych? Kiedy pracownicy mieli ostatnie szkolenie w tym zakresie? |  |  |
| Czy pracownicy podmiotu przetwarzającego, którzy uczestniczą w operacjach przetwarzania danych osobowych, zostali zobowiązani na piśmie do zachowania ich w tajemnicy? |  |  |
| Czy podmiot przetwarzający stosuje zatwierdzony kodeks postępowania, o którym mowa w art. 40 Rozporządzenia, lub zatwierdzony mechanizm certyfikacji, o którym mowa w art. 42 Rozporządzenia? |  |  |
| Czy w ciągu dwóch ostatnich lat podmiot przetwarzający poddawał zewnętrznej lub wewnętrznej kontroli niezależnych audytorów funkcjonujący w jego organizacji system ochrony danych osobowych? Jeżeli tak to kiedy i jakie były zalecenia |  |  |
| Czy podmiot przetwarzający korzysta z usług tylko takich podmiotów zewnętrznych / podwykonawców, którzy zostali wcześniej przez niego sprawdzeni pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych? Jeżeli tak, to w jaki sposób? |  |  |
| Czy podmiot przetwarzający zastosował środki kontroli dostępu fizycznego do budynku/budynków tylko dla autoryzowanego personelu? Jeżeli tak to jakie to środki? |  |  |
| Czy podmiot przetwarzający zapewnił fizyczne oddzielenie środków przetwarzania informacji zarządzanych przez jego organizację od tych, które należą do innych organizacji? Np. osobne biura, osobna sieć, prosimy o wskazanie |  |  |
| Czy dostęp do pomieszczeń pozostających w dyspozycji podmiotu przetwarzającego po godzinach pracy nie jest możliwy dla osób trzecich (firma sprzątająca, ochrona) bądź dostęp ten jest szczegółowo nadzorowany? Jeżeli jest monitorowany to w jaki sposób? |  |  |
| Czy każdy pracownik podmiotu przetwarzającego otrzymuje imienny identyfikator do systemów informatycznych? |  |  |
| Czy stosowane systemy informatyczne zapewniają bezpieczeństwo przetwarzanych danych przed nieautoryzowanym dostępem np.. Poprzez stosowanie MFA, 2FA, generatory i menagery haseł? Jeżeli tak to jakie mechanizmy są stosowane? |  |  |
| Czy pracownicy podmiotu przetwarzającego zostali zobowiązani do zabezpieczania nieużywanych w danym momencie systemów przez blokadę ekranu lub w inny równoważny sposób? |  |  |
| Czy w organizacji podmiotu przetwarzającego jest stosowana polityka czystego biurka? |  |  |
| Czy podmiot przetwarzający zapewnił oprogramowanie antywirusowe na wszystkich stacjach? |  |  |
| Czy oprogramowanie ma licencję i jest na bieżąco aktualizowane? |  |  |
| Czy podmiot przetwarzający stosuje szyfrowanie dysków komputerów przenośnych? |  |  |
| Czy urządzenia mobilne mają skonfigurowaną kontrolę dostępu? |  |  |
| Czy podmiot przetwarzający stosuje szyfrowanie dysków na urządzeniach mobilnych? |  |  |
| Czy na urządzeniach mobilnych jest stosowane oprogramowanie antywirusowe? |  |  |
| Czy zapewniono zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego? Jeżeli tak to w jaki sposób? |  |  |
| Jaki przyjęto zakres oraz jaką częstotliwość tworzenia kopii zapasowych?  |  |  |
| Gdzie są przechowywane kopie zapasowe? |  |  |
| Czy podmiot przetwarzający posiada procedury odtwarzania systemu po awarii oraz ich testowania? |  |  |
| Czy podmiot przetwarzający wdraża nowe rozwiązania zgodnie z zasadą privacy by design? |  |  |
| Czy podmiot przetwarzający działa zgodnie z zasadą privacy by default? |  |  |
| Czy podmiot przetwarzający prowadzi ocenę skutków dla ochrony danych? Jeżeli była wymagana w jego działalności |  |  |
| Czy podmiot przetwarzający gwarantuje realizację praw osób, których dane dotyczą, tj. m.in. prawo do przenoszenia danych, prawo do ograniczenia przetwarzania, prawo do bycia zapomnianym? Jeżeli tak to w jaki sposób? |  |  |

data i podpis Podmiotu Przetwarzającego