Załącznik nr 1 do UPPDO

**Arkusz weryfikacji podmiotu przetwarzającego**

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), w skrócie RODO

**Art. 28 ust. 1 RODO**

*„Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą”.*

Motyw 81 RODO

„*Aby zapewnić przestrzeganie wymogów niniejszego rozporządzenia w przypadku przetwarzania, którego w imieniu administratora ma dokonać podmiot przetwarzający, administrator powinien, powierzając podmiotowi przetwarzającemu czynności przetwarzania, korzystać z usług wyłącznie podmiotów przetwarzających, które zapewniają wystarczające gwarancje - w szczególności jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby - wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom niniejszego rozporządzenia, w tym wymogom bezpieczeństwa przetwarzania…”.*

|  |  |
| --- | --- |
| Dane (potencjalnego) podmiotu przetwarzającego (nazwa, siedziba, NIP, REGON, KRS) |  |
| Przedmiot umowy, zakres współpracy |  |

**Wykaz środków organizacyjnych i technicznych stosowanych przez Podmiot przetwarzający**

|  |  |
| --- | --- |
| **PYTANIE** | **ODPOWIEDŹ** |
| Czy 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 zapewnia, że każdy 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? |  |
| Czy przetwarzający zapewnia, że wszyscy jego pracownicy zaangażowani w operacje przetwarzania danych osobowych posiadają pisemne upoważnienia do przetwarzania danych osobowych? |  |
| Czy pracownicy podmiotu przetwarzającego, którzy uczestniczą w operacjach przetwarzania danych osobowych, zostali zobowiązani do zachowania ich w tajemnicy? |  |
| Czy podmiot realizując swoją działalność przeprowadza procesy przetwarzania danych w innych krajach? Jeśli tak, proszę wskazać gdzie. |  |
| Czy w celu realizacji umowy niezbędne okaże się przekazanie danych administratora do innego kraju UE lub do państwa trzeciego?  Jeśli tak, proszę wskazać gdzie. |  |
| Czy realizując przedmiotową umowę podmiot będzie korzystał z usług innych wykonawców?  Jeżeli tak, proszę wskazać te podmioty.  Dotyczy to również sytuacji związanych z hostingiem, serwisem technicznym. |  |
| Czy inni wykonawcy, z których usług korzysta podmiot, a przetwarzający dane administratora zostali przez niego sprawdzeni pod kątem bezpieczeństwa danych osobowych?  Jeśli tak, proszę wskazać sposób dokonania sprawdzenia. |  |
| Czy podmiot realizując swoją działalność obsługiwał lub obsługuje podmioty, z którymi ma zawarte umowy powierzenia przetwarzania danych? |  |
| Czy w ciągu dwóch ostatnich lat podmiot przetwarzający poddawał zewnętrznej kontroli niezależnych audytorów funkcjonujący w jego organizacji system ochrony danych osobowych? |  |
| 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? |  |
| Czy przetwarzający opracował i wdrożył procedurę dotyczącą sposobu działania w przypadku wystąpienia incydentu naruszenia danych osobowych? Proszę o wskazanie nazwy ww. dokumentu wraz z datą zatwierdzenia oraz nadanym numerem wewnętrznym. |  |
| Czy podmiot przetwarzający zastosował środki kontroli dostępu fizycznego do budynku/budynków tylko dla autoryzowanego personelu? |  |
| Czy podmiot przetwarzający zapewnił fizyczne oddzielenie środków przetwarzania informacji zarządzanych przez jego organizację od tych, które należą do innych organizacji? |  |
| 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? |  |
| Czy każdy pracownik podmiotu przetwarzającego otrzymuje imienny identyfikator do systemów informatycznych? |  |
| Czy systemy informatyczne zapewniają wymuszanie na użytkownikach okresowych zmian haseł oraz zmian w razie zaistniałej potrzeby? |  |
| Czy pracownicy podmiotu przetwarzającego zostali zobowiązani do zabezpieczania nieużywanych w danym momencie systemów przez blokadę ekranu lub w inny równoważny sposób? |  |
| Czy pracownicy podmiotu przetwarzającego zostali zobowiązani do niezwłocznego odbierania z drukarek wydruków zawierających dane osobowe lub inne poufne informacje? Czy wskazana zasada jest przestrzegana przez pracowników? |  |
| Czy w organizacji podmiotu przetwarzającego jest stosowana polityka czystego biurka? |  |
| Czy dane osobowe gromadzone w formie papierowej są przechowywane, po godzinach pracy organizacji podmiotu przetwarzającego, w zamykanych szafach/szafkach/szufladach bez możliwości dostępu do nich osób nieupoważnionych? |  |
| 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 techniki kryptograficzne wobec urządzeń mobilnych? |  |
| Czy na urządzeniach mobilnych zainstalowano oprogramowanie antywirusowe? |  |
| Czy zapewniono zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego? |  |
| Jaki przyjęto zakres oraz jaką częstotliwość tworzenia kopii zapasowych i gdzie są przechowywane? |  |
| 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? |  |
| Czy przetwarzający opracował i wdrożył procedurę umożliwiającą realizację praw osób, których dane osobowe dotyczą? Proszę o wskazanie nazwy ww. dokumentu wraz z datą zatwierdzenia oraz nadanym numerem wewnętrznym. |  |
| 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? |  |

*………………………………………………………………………………………………………………..*

*Data i podpis osoby reprezentującej (potencjalny) podmiot przetwarzający*