**Załącznik nr 1c do Procedury wyboru kontrahenta**

Lista pytań kontrolnych w zakresie weryfikacji zapewniania wymogów przez potencjalnego kontrahenta. Ankieta należąca do: Samodzielny Publiczny Zakład Opieki Zdrowotnej MSWiA w Krakowie jako administratora danych osobowych przekazywana potencjalnemu kontrahentowi, któremu zostaną powierzone dane osobowe.

|  |  |
| --- | --- |
| **Dokumentacja dotycząca ochrony danych** | |
| Czy Wykonawca/Dostawca wyznaczył u siebie Inspektora ochrony danych? Jakie kwalifikacje i doświadczenie zawodowe posiada IOD? |  |
| Czy zgodnie z art. 29 RODO osoby wykonujące operacje na danych osobowych otrzymały od Wykonawcy/Dostawcy upoważnienia do przetwarzania danych, w których został określony zakres przetwarzanych przez te osoby danych? |  |
| Czy Wykonawca/Dostawca prowadzi Rejestr kategorii czynności przetwarzania danych zgodnie z art. 30 ust. 2 RODO? |  |
| Czy Wykonawca/Dostawca posiada dokumentację opisującą przetwarzanie danych: Polityki, Instrukcje, Procedury na podstawie, których jest w stanie wykazać zapewnienie bezpieczeństwa przetwarzanych danych? |  |
| Czy Wykonawca/Dostawca przeprowadza szkolenia z ochrony danych/prawidłowego postępowania z danymi osobowymi dla nowozatrudnionych osób przystępujących do pracy? |  |
| Czy osoby przeszkolone potwierdzają pisemnie fakt zapoznania się z przepisami RODO oraz wewnętrznymi Politykami, Instrukcjami, Regulaminami obowiązującymi u Wykonawcy/Dostawcy? |  |
| Czy Wykonawca/Dostawca przeprowadza cykliczne szkolenia lub prowadzi inne działania mające na celu podnoszenie poziomu świadomości wśród osób zatrudnionych w zakresie zagadnień dotyczących ochrony danych osobowych? |  |
| Czy osoby zatrudnione u Wykonawcy/Dostawcy podpisały Oświadczenia o poufności/ Zobowiązania do zachowania tajemnicy? |  |
| Czy i jak często wykonywane są audyty u Wykonawcy/Dostawcy związane z ochroną danych? |  |
| Czy Wykonawca/Dostawca poddaje się zewnętrznej kontroli niezależnych audytorów w zakresie funkcjonującego systemu bezpieczeństwa danych? |  |
| Czy Wykonawca/Dostawca korzysta z usług podmiotów zewnętrznych/ podwykonawców? Czy sprawdził ich pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych? |  |
| Czy dane gromadzone w formie papierowej, po godzinach pracy, przechowywane są w taki sposób, aby nie miały do nich dostępu osoby nieupoważnione? Np. w zamykanych szafach, biurkach itp. |  |
| Czy u Wykonawcy/Dostawcy stosowana jest zasada „czystego biurka”? |  |
| Czy Wykonawca/Dostawca wprowadził Procedurę niszczenia dokumentów? Czy zakupiono odpowiedni sprzęt spełniający wymagania bezpiecznego niszczenia dokumentów lub podpisano umowę powierzenia przetwarzania danych z firmą zajmującą się niszczeniem dokumentów? |  |
| Czy Wykonawca/Dostawca posiada Procedurę realizacji praw osób fizycznych i gwarantuje na jej podstawie realizację podstawowych praw, takich jak: prawo dostępu, żądania prawa do ograniczenia danych, żądanie prawa do bycia zapomnianym, itp.? |  |
| Czy Wykonawca/Dostawca posiada Procedurę dotyczącą postępowania w momencie wystąpienia incydentu naruszenia bezpieczeństwa danych? |  |
| Czy Wykonawca/Dostawca posiada Procedurę zgłaszania naruszeń bezpieczeństwa danych Organowi Nadzorczemu? |  |
| Czy Wykonawca/Dostawca wykonał analizę ryzyka w obszarach przetwarzanych danych najbardziej narażonych na niebezpieczeństwo? |  |
| Czy Wykonawca/Dostawca posiada Procedurę privacy by design i zgodnie z tą procedurą wdraża nowe rozwiązania oraz Procedurę privacy by default i działa zgodnie z jej zasadami? |  |
| Czy Wykonawca/Dostawca był kiedykolwiek kontrolowany przez Organ Nadzorczy lub inny organ publiczny w związku z przetwarzaniem danych osobowych? Z jakim wynikiem? |  |
| Czy Wykonawca/Dostawca wypełnia obowiązki informacyjne zgodnie z art. 13 i 14 RODO? |  |
| **Dostęp fizyczny do budynków/pomieszczeń/dokumentacji** | |
| Czy w siedzibie Wykonawcy/Dostawcy stosowane są środki kontroli dostępu fizycznego do budynków/ pomieszczeń? Czy dostęp mogą mieć tylko autoryzowane osoby zatrudnione/ goście po uprzedniej weryfikacji? |  |
| Czy Wykonawca/Dostawca posiada dokument opisujący dostęp do budynków/pomieszczeń, np. Procedurę wydawania kluczy lub tym podobne? |  |
| Czy dostęp do pomieszczeń Wykonawcy/Dostawcy po wyznaczonych godzinach pracy jest szczegółowo nadzorowany? |  |
| Czy zewnętrzne firmy, np. firma sprzątająca, firma obsługująca monitoring itd. ma dostęp do pomieszczeń Wykonawcy/Dostawcy po wyznaczonych godzinach pracy wyłącznie pod nadzorem? Czy osoby zatrudnione w takiej firmie mają podpisane Zobowiązania do zachowania tajemnicy? |  |
| Czy zewnętrzne firmy, np. firma obsługująca monitoring ma dostęp wyłącznie do bieżącego podglądu w systemie monitoringu? |  |
| Czy Wykonawca/Dostawca wyznaczył osoby odpowiedzialne za dostęp do systemu monitoringu z możliwością nagrywania? Czy osoby te mają pisemne upoważnienia w tym zakresie? |  |
| Czy Wykonawca/Dostawca posiada Procedurę udostępniania nagrań z systemu monitoringu? |  |
| **System informatyczny** | |
| Czy każda osoba zatrudniona u Wykonawcy/Dostawcy przetwarzająca dane w systemie informatycznym otrzymuje własny login i hasło? |  |
| Czy system informatyczny Wykonawcy/Dostawcy zapewnia wymuszenie na użytkownikach okresowe zmiany haseł oraz zmiany w razie zaistniałej potrzeby? |  |
| Czy osoby zatrudnione u Wykonawcy/Dostawcy zostały przeszkolone w zakresie tworzenia haseł odpowiednio silnych chroniących dostęp do systemy/aplikacji, w których przetwarzane są dane? |  |
| Czy system informatyczny Wykonawcy/Dostawcy zapewnia zabezpieczenie chwilowo nieużywanych aplikacji poprzez blokadę ekranu lub w inny równoważny sposób? |  |
| Czy osoby zatrudnione u Wykonawcy/Dostawcy zostały uświadomione, że nie powinny pozostawiać bez nadzoru swojego stanowiska pracy, a w razie takiej konieczności są zobowiązane zastosować blokadę ekranu lub inny równoważny system? |  |
| Czy Wykonawca/Dostawca stosuje podstawowe środki wymienione w art. 32 np. pseudonimizację, szyfrowanie, itp.? |  |
| Czy osoby zatrudnione u Wykonawcy/Dostawcy zostały przeszkolone w zakresie bezpiecznego użytkowania elektronicznej poczty służbowej? Bezpiecznego sposobu wysyłania wiadomości e-mail zawierających dane osobowe? |  |
| Czy osoby zatrudnione u Wykonawcy/Dostawcy zostały przeszkolone w zakresie bezpiecznego użytkowania przenośnych urządzeń zawierających dane osobowe, np. laptopów, telefonów komórkowych, itp.? |  |
| Czy osoby zatrudnione u Wykonawcy/Dostawcy zostały przeszkolone w zakresie bezpiecznego użytkowania Internetu w celach służbowych? |  |
| Czy Wykonawca/Dostawca korzysta z usług hostingu? Czy podpisał w tym zakresie umowę powierzenia przetwarzania danych osobowych? |  |
| Czy oprogramowanie stosowane u Wykonawcy/Dostawcy posiada licencję i jest na bieżąco aktualizowane? |  |
| Czy zapewniono oprogramowanie antywirusowe na wszystkich stacjach? |  |
| Czy stosuje się szyfrowanie dysków komputerów przenośnych? |  |
| Czy urządzenia przenośne posiadają skonfigurowaną kontrolę dostępu? |  |
| Czy na urządzeniach mobilnych zainstalowano oprogramowanie antywirusowe? |  |
| Czy Wykonawca/Dostawca tworzy kopie zapasowe przetwarzanych danych? |  |
| Gdzie Wykonawca/Dostawca przechowuje kopie zapasowe? |  |
| Czy Wykonawca/Dostawca wykonuje testy kopii bezpieczeństwa i jak często? |  |
| Czy Wykonawca/Dostawca prowadzi rejestr przeprowadzanych testów kopii bezpieczeństwa? |  |

………………………………………………………...

miejscowość i data

......................................................................................................

imię i nazwisko oraz podpis osoby reprezentującej Kontrahenta