ZAŁĄCZNIK NR 8 – OŚWIADCZENIE O SPEŁNIENIU MINIMALNYCH WYMAGAŃ W ZAKRESIE STOSOWANYCH ZABEZPIECZEŃ TECHNICZNYCH I ORGANIZACYJNYCH DOTYCZĄCYCH OCHRONY DANYCH OSOBOWYCH OSÓB FIZYCZNYCH PO MODYFIKACJI

|  |  |
| --- | --- |
| **OŚWIADCZENIE WYKONAWCY** | |
| (pieczęć Wykonawcy) |  | |

**Dotyczy:**

**Świadczenie Usług SAP Enterprise Support w odniesieniu do Oprogramowania SAP w GK ENEA**

**w okresie od 01.01.2022r. do 31.12.2022r.**

**Oznaczenie Sprawy: 1400/DW00/ZT/KZ/2021/0000098116**

Niniejszym oświadczam(y), że reprezentowany przeze mnie (przez nas) podmiot spełnia następujące minimalne wymagania w zakresie stosowanych zabezpieczeń technicznych i organizacyjnych dotyczących ochrony danych osobowych osób fizycznych:

X - oznacza wymagania konieczne do wystartowania w postępowaniu

Pole puste w kolumnie *minimalne wymagania, które Wykonawca zobowiązany jest spełnić* oznacza wymagania których spełnienie jest mile widziane ale ich brak nie dyskwalifikuje z udziału w postępowaniu

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Obszary wymagań** | | **Rodzaje zabezpieczeń** | **Minimalne wymagania, które Wykonawca zobowiązany jest spełnić[[1]](#footnote-2)** | **W przypadku spełniania warunków proszę wpisać V** |
| środki organizacyjne | zabezpieczenia proceduralne  i osobowe | polityki, procedury, instrukcje, | x |  |
| stosuje się do ogólnych zasad przetwarzania określonych w art. 5 RODO, | x |  |
| zapewnia, aby dane przetwarzane były zgodnie z prawem – art. 6 – 11 RODO, | x |  |
| zapewnia, aby przestrzegane były prawa osób, których dane są przetwarzane – art. 12-23 RODO | x |  |
| zapewnia wypełnianie ogólnych obowiązków w zakresie przetwarzania danych ciążących na administratorze i podmiocie przetwarzającym – art. 24 – 31 RODO, | x |  |
| zapewnia bezpieczeństwo przetwarzania danych uwzględniając charakter zakres, kontekst i cele przetwarzania danych – art. 32- 36 RODO, | x |  |
| zapewnia kontrolę nad przetwarzaniem danych w postaci monitorowania przestrzegania przepisów i przyjętych procedur przetwarzania przez Inspektora Ochrony Danych lub podmioty certyfikujące, czy monitorujące przestrzeganie przyjętych kodeksów postepowania – art. 27- 43 RODO, | x |  |
| certyfikacja RODO |  |  |
| oświadczenia o zachowaniu bezpieczeństwa , |  |  |
| procedury dotyczące zgłaszanie naruszeń ochrony danych do organu nadzorczego (UODO) – art. 33 ust 3 RODO; | x |  |
| procedury dotyczące prowadzenia wewnętrznego rejestru naruszeń ochrony danych, o którym mowa w art. 33 ust 5 RODO; |  |  |
| wyznaczono IOD zgodnie z  art. 37RODO |  |  |
| raporty dokumentujące wyniki przeprowadzonych ocen skutków dla ochrony danych – art. 35 ust. 7. |  |  |
| kodeksy branżowe/ stowarzyszenia branżowe |  |  |
| upoważnienia do przetwarzania danych osobowych oraz ewidencja upoważnień | x |  |
| umowy powierzenia z podwykonawcami oraz ewidencja umów powierzenia przetwarzania | x |  |
| zarządzanie aktywami (przetwarzanymi zbiorami danych), | x |  |
| w ciągu ostatnich 24 miesięcy działalność podmiotu została skontrolowana przez właściwe, ze względu na przedmiot działalności danego podmiotu, instytucje zewnętrzne, np. inspekcja pracy, UODO |  |  |
| wdrożono zalecenia z w/w kontroli w całości |  |  |
| wdrożono zalecenia z w/w kontroli częściowo |  |  |
| nie wdrożono zalecenia z w/w kontroli |  |  |
| zaimplementowano klasyfikację informacji. |  |  |
| zaimplementowano postępowanie z informacją. | x |  |
| zaimplementowano obsługę incydentów dot. ochrony danych osobowych. |  |  |
| zarządzanie ryzykiem przetwarzania danych osobowych | x |  |
| środki techniczne | zabezpieczenia teleinformatyczne | kontrole dostępu (rejestrowanie i wyrejestrowywanie użytkowników, zarządzanie hasłami, użycie uprzywilejowanych programów narzędziowych | x |  |
| informuje się Zamawiającego o incydencie naruszenia bezpieczeństwa teleinformatycznego, jeśli dotyczy on usług wykonywanych dla Zamawiającego | x |  |
| autoryzacja i autentykacja, |  |  |
| system UPS |  |  |
| redundancja – dublowanie elementów systemu |  |  |
| generatory prądu |  |  |
| testowanie systemów i procesów |  |  |
| kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa; |  |  |
| licencje na legalność oprogramowania, | x |  |
| systemy antywirusowe, | x |  |
| systemy antyspamowe, | x |  |
| zapory, | x |  |
| wykonywanie  kopii bezpieczeństwa, wszystkich stacji roboczych |  |  |
| wykonywanie kopii bezpieczeństwa całego serwera poczty elektronicznej |  |  |
| wykonywanie kopii bezpieczeństwa danych przetwarzanych w imieniu Zamawiającego | x |  |
| miejsce przechowywania kopii zapasowej jest różne od lokalizacji produkcyjnej. |  |  |
| stosowanie okresowego testowego odtwarzania wybranych kopii zapasowych na potrzeby weryfikacji poprawności |  |  |
| Dostawca przesyła załączniki zawierające informacje wrażliwe dla Zlecającego (np. dane konfiguracyjne, logi, dane osobowe) w postaci archiwum (np. zip/7z), zaszyfrowanego z użyciem szyfru AES min. 256 i zabezpieczonego silnym hasłem (co najmniej 10 znaków, kombinacja cyfr, wielkich i małych liter oraz symboli specjalnych, nie zawiera całego wyrazu słownikowego, nie zawiera powtórzeń znaków, ani ciągów znaków występujących obok siebie na klawiaturze). Hasła do archiwum są przesyłane innym kanałem niż plik archiwum.  Dla uniknięcia wątpliwości powyższy wymóg nie ma zastosowania do poniższego katalogu informacji przekazywanych przez Wykonawcę/producenta oprogramowania SAP, które Wykonawca udostępni wskazanym pracownikom Zamawiającego) na określonych zasobach, do których link zostanie przesłany w wiadomości email (identyfikatory i hasła są tworzone przez Zamawiającego we własnym zakresie na portalu udostępnionym przez Wykonawcę):  • Raporty z usług SAP Continous Quality Checks  Opis usługi:  https://support.sap.com/en/offerings-programs/enterprisesupport/enterprise-support-academy/continuous-quality-checkimprovement-services.html  Dodatkowo powyższym wymogiem nie są objęte raporty, które są generowane tylko na zamówienie Zamawiającego na dedykowanych przez producenta oprogramowania SAP witrynach internetowych (zamawiając taki raport Zamawiający akceptuje warunki jego dostarczenia określone na witrynie internetowej) na przykład:  • Raport Pathfinder  Opis usługi:  https://support.sap.com/en/release-upgrade-maintenance/valuesupport/quick-values-pathfinder.html  • Raport Support Insights Report (SIR)  • Raport EarlyWatch Alert  • Raport S/4HANA Readiness Check  Opis usługi: https://help.sap.com/viewer/product/SAP\_READINESS\_CHECK/200/en-US  • Process Discovery  Opis usługi:  https://bpi-discoveryproxy.cfapps.eu10.hana.ondemand.com/request/BSN/  Powyższy wymóg nie ma zastosowania do poniższego zakresu (jeśli informacje nie zawierają danych wrażliwych dla Zamawiającego:   * Odpowiedzi na pytania przesłane przez Zamawiającego emailem. * Prezentacje/materiały przygotowane wspólnie z Zamawiającym w celach referencyjnych (np. opracowanie materiałów podsumowujących korzyści osiągnięte z korzystania z umowy SAP Enterprise Support).   Z zastrzeżeniem, iż w podsumowaniach dotyczących przeglądu systemu Zamawiającego mogą znajdować się zrzuty ekranowe z raportu Early Watch Alert zwierające szczątkowe dane konfiguracyjne.  Dla pozostałych załączników lub informacji przesyłanych drogą elektroniczną, które nie zawierają informacji wrażliwych dla Zamawiającego (np. informacje marketingowe, komunikaty nie zawierające informacji wrażliwych) można odstąpić od szyfrowania plików lub wiadomości email. | x |  |
| szyfrowanie, | x |  |
| bezpieczne łącza, | x |  |
| pseudonimizacja, |  |  |
| zabezpieczenie logów systemów, | x |  |
| środki ochrony kryptograficznej (polityka stosowania zabezpieczeń, zarządzanie kluczami |  |  |
| segmentacja i separacja sieci, | x |  |
| stosowanie własnej domeny firmowej |  |  |
| tworzenie konta na domenie dla pracowników Wykonawców oraz ich podwykonawców |  |  |
| korzystanie z własnego serwera poczty elektronicznej. |  |  |
| korzystanie z podpisu cyfrowego w poczcie elektronicznej dla wiadomości elektronicznych |  |  |
| korzystanie z podpisu cyfrowego w poczcie elektronicznej dla załączników. |  |  |
| nie korzystanie z chmur publicznych (np. AWS, GCP, Azure) i publicznych zasobów plikowych (np. DropBox, Google Drive, OneDrive) do wykonywania powierzonych przez ENEA zadań. Wyjątek stanowi sytuacja, gdy w umowie Wykonawca odpowiada za działania podwykonawców/dostawców jak za własne, a w umowie widnieje zapis o odpowiedzialności finansowej dot. w/w odpowiedzialności, której wysokość jest akceptowana przez Zamawiającego (właściciela biznesowego danego systemu od strony Zamawiającego). | x |  |
| zapewnia się, że zdalny dostęp jest możliwy tylko przez bezpieczne połączenia | x |  |
| nie podłącza się niedozwolonych urządzeń (bez zgody Zamawiającego) do sieci LAN Zamawiającego (za wyjątkiem dostępu jako gość) | x |  |
| zabezpieczenia fizyczne | monitoring wizyjny, |  |  |
| monitoring wizyjny w trybie ciągłym |  |  |
| monitoring wizyjny w trybie okresowym |  |  |
| bezpieczeństwo fizyczne i środowiskowe oraz bezpieczeństwo eksploatacji (zarządzanie zmianami, zarządzanie pojemnością, zapewnienie ciągłości działania, rejestrowanie zdarzeń i monitorowanie |  |  |
| monitoring elektroniczny kontrola dostępu, |  |  |
| ochrona fizyczna obiektów, |  |  |
| systemy antywłamaniowe, |  |  |
| działanie grup interwencyjnych, |  |  |

|  |  |
| --- | --- |
|  |  |
| **miejscowość i data** | **podpis przedstawiciela(i) Wykonawcy** |

1. Minimalne wymagania, które jest zobowiązany spełnić Wykonawca zostały oznaczone w następujący sposób: X [↑](#footnote-ref-2)