**ZAŁĄCZNIK NR 5 – OŚWIADCZENIE O SPEŁNIENIU MINIMALNYCH WYMAGAŃ W ZAKRESIE STOSOWANYCH ZABEZPIECZEŃ TECHNICZNYCH I ORGANIZACYJNYCH DOTYCZĄCYCH OCHRONY DANYCH OSOBOWYCH OSÓB FIZYCZNYCH PO MODYFIKACJI**

|  |  |
| --- | --- |
| (nazwa Wykonawcy) |  |

**Dostawa materiałów promocyjnych dla ENEA S.A.**

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) |
| środki organizacyjne | zabezpieczenia proceduralne  i osobowe | polityki, procedury, instrukcje, |  |
| 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 , | X |
| procedury dotyczące zgłaszanie naruszeń ochrony danych do organu nadzorczego (UODO) – art. 33 ust 3 RODO; |  |
| procedury dotyczące prowadzenia wewnętrznego rejestru naruszeń ochrony danych, o którym mowa w art. 33 ust 5 RODO; |  |
| wyznaczono IOD zgodnie z art. 37RODO | x |
| 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), |  |
| 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. |  |
| zaimplementowano obsługę incydentów dot. ochrony danych osobowych. |  |
| zarządzanie ryzykiem przetwarzania danych osobowych |  |
| środki techniczne | zabezpieczenia teleinformatyczne | systemy antywirusowe, antyspamowe, antymalwareowe |  |
| licencje na legalność oprogramowania, |  |
| autoryzacja i autentykacja, |  |
| kontrole dostępu (rejestrowanie i wyrejestrowywanie użytkowników, zarządzanie hasłami, użycie uprzywilejowanych programów narzędziowych) |  |
| Szyfrowanie (np. szyfrowanie pliku/plików zawierających wrażliwe dane w przypadku ich przesyłania/wymiany; może być to wykonane poprzez spakowanie i zahasłowanie pliku/plików silnym hasłem o długości min. 12 znaków), |  |
| bezpieczne łącza, |  |
| pseudonimizacja, |  |
| zapory, |  |
| zabezpieczenie logów systemów, |  |
| środki ochrony kryptograficznej (polityka stosowania zabezpieczeń, zarządzanie kluczami) |  |
| segmentacja i separacja sieci, |  |
| nie będą wykorzystywane chmury publiczne (np. AWS, GCP, Azure) i publiczne zasoby plikowe (np. DropBox, Google Drive, OneDrive) do wykonywania zadań powierzonych przez Zamawiającego dla informacji wrażliwych (np. danych osobowych, logów, plików konfiguracyjnych, informacji zarządczych), jedynie za zgodą strony biznesowej Zamawiającego |  |
| Dostawca zapewnia, że zdalny dostęp jest możliwy tylko przez bezpieczne połączenia |  |
| nie podłączanie niedozwolonych urządzeń (bez zgody Zamawiającego) do sieci LAN Zamawiającego (za wyjątkiem dostępu jako gość) |  |
| Wykonawca stosuje w swoich sieciach bezprzewodowych (np. wifi) standard 802.1X (gdy nie korzysta z VPN Zamawiającego). |  |
| 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 | X |
| monitoring elektroniczny kontrola dostępu, |  |
| ochrona fizyczna obiektów, |  |
| systemy antywłamaniowe, | X |
| 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)