**Ankieta Zgodności Podmiotu Przetwarzającego**

**z wymaganiami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r.**

|  |  |
| --- | --- |
| **Nazwa podmiotu przetwarzającego** |  |
| **Adres podmiotu przetwarzającego** |  |
| **Dane kontaktowe** |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| PYTANIA DOTYCZĄCE kwestii organizacyjnych | | | TAK | | NIE | | NIE DOTYCZY | | | Uwagi | | Ocena\* |
| 1. | Czy zgodnie z art. 29 RODO osoby przetwarzające dane osobowe w imieniu i na polecenie Podmiotu Przetwarzającego otrzymały upoważnienia do przetwarzania tych danych, z wyszczególnieniem zakresu przetwarzania | |  | |  | |  | | |  | |  |
| 2. | Czy osoby przetwarzające dane w imieniu i na polecenie Podmiotu Przetwarzającego zobowiązały się do zachowania w poufności tych danych oraz sposobów ich przetwarzania? | |  | |  | |  | | |  | |  |
| 3. | Czy Podmiot Przetwarzający wyznaczył Inspektor Ochrony Danych (dalej: IOD)? | |  | |  | |  | | |  | |  |
| Jeżeli TAK, proszę podać imię i nazwisko oraz dane kontaktowe IOD. | |  | | | | | | | | |  |
| 4. | W przypadku braku konieczności powołania IOD – czy Podmiot Przetwarzający wyznaczył osobę odpowiedzialną za ochronę danych osobowych? | |  | |  | |  |  | | | |  |
| Jeżeli TAK, proszę podać imię i nazwisko oraz dane kontaktowe osoby, która jest odpowiedzialna za ochronę danych osobowych. | |  | |  | |  |  | | | |  |
| 5. | Czy Podmiot Przetwarzający realizuje wymagania art. 30 ust. 2 RODO (czy prowadzi rejestr kategorii czynności przeważania)? | |  | |  | |  |  | | | |  |
| 6. | Czy Podmiot Przetwarzający opracował politykę ochrony danych lub inną dokumentację opisującą zasady ochrony danych osobowych? | |  | |  | |  |  | | | |  |
| 7. | Czy Podmiot Przetwarzający zapewnia, że nowozatrudniony pracownik przed podjęciem czynności związanych z przetwarzaniem danych osobowych został odpowiednio przeszkolony w tym zakresie oraz zapoznany z obowiązującymi przepisami prawa? | |  | |  | |  |  | | | |  |
| 8. | Czy podmiot Przetwarzający dba o doskonalenie wiedzy swoich pracowników w zakresie ochrony danych osobowych poprzez cykliczne szkolenia? | |  | |  | |  |  | | | |  |
| 9. | Czy Podmiot Przetwarzający stosuje zatwierdzony kodeks postepowania, o którym mowa a art. 40 lub zatwierdzony mechanizm certyfikacji, o którym mowa w art. 42? | |  | |  | |  |  | | | |  |
| 10. | Czy Podmiot Przetwarzający korzysta z usług tylko takich podmiotów zewnętrznych/podwykonawców, którzy gwarantują odpowiednie bezpieczeństwo danych osobowych (zgodność z RODO) oraz czy te podmioty zostały przez niego zweryfikowane? | |  | |  | |  |  | | | |  |
| 11. | Czy Podmiot Przetwarzający podpisał stosowne umowy powierzenia z podwykonawcami? | |  | |  | |  |  | | | |  |
| 12. | Czy w ciągu ostatnich dwóch lat Podmiot Przetwarzający przeprowadził kompleksowy audyt zgodności z przepisami o ochronie danych osobowych? | |  | |  | |  |  | | | |  |
| 13. | Czy Podmiot Przetwarzający wdraża nowe rozwiązania w oparciu o zasadę „privacy by design”? | |  | |  | |  | | |  | |  |
| 14. | Czy Podmiot Przetwarzający działa zgodnie z zasadą „privacy by default”? | |  | |  | |  | | |  | |  |
| 15. | Czy Podmiot Przetwarzający wypracował zasady realizacji praw Podmiotów Danych w zakresie ochrony danych osobowych, o którym mowa w art. 15-22 RODO | |  | |  | |  | | |  | |  |
| 16. | Czy Podmiot Przetwarzający oszacował ryzyko przetwarzania danych osobowych? | |  | |  | |  | | |  | |  |
| 17. | Czy Podmiot Przetwarzający dokonała oceny skutków dla ochrony danych osobowych dla czynności przetwarzania (o których mowa w art. 35 RODO i w wykazie rodzajów operacji przetwarzania danych wymagających oceny skutków dla ochrony ich danych, opublikowanym w komunikacie Prezesa Urzędu Ochrony Danych Osobowych), a które wchodzą w zakres planowanej? | |  | |  | |  | | |  | |  |
| PYTANIA DOTYCZĄCE BEZPIECZEŃSTWA FIZYCZNEGO | | |  | |  | |  | | |  | |  |
| 18. | Czy Podmiot Przetwarzający opracował procedury dotyczące nadawania fizycznego dostępu do pomieszczeń, w których przechowywana jest dokumentacja zawierająca dane osobowe, zapewniające weryfikację tożsamości i zakres nadawanego dostępu? | |  | |  | |  | | |  | |  |
| 19. | Czy istnieją mechanizmy kontroli dostępu to tych pomieszczeń? | |  | |  | |  | | |  | |  |
| 20. | 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? | |  | |  | |  | | |  | |  |
| 21. | Czy Podmiot Przetwarzający posiada działający system alarmowy oraz system monitoringu przemysłowego obejmujący miejsca, gdzie przechowywana jest dokumentacja medyczna oraz inne dane osób fizycznych? | |  | |  | |  | | |  | |  |
| PYTANIE DOTYCZĄCE STSOWANYCH ŚRODKÓW BEZPIECZEŃSTWA W ŚRODOWISKU INFORMATYCZNYM | |  | | |  | |  | | |  | |  |
| 22. | Czy Podmiot Przetwarzający zapewnia jednoznaczną identyfikację działań w systemach informatycznych za pomocą unikalnego ID Użytkownika? | |  | |  | |  | | |  | |  |
| 23. | Czy system, w którym są przetwarzane dane osobowe posiada funkcjonalności pozwalające na jednoznaczne wskazanie i odtworzenie działań użytkownika o konkretnym ID, w określonym czasie? | |  | |  | |  | | |  | |  |
| 24 | Czy Podmiot Przetwarzający posiada formalne zasady zarządzania hasłami (minimalna długość, złożoność, częstotliwość zmiany, możliwość powtórnego użycia hasła, szyfrowanie przechowywanych haseł), które są wdrożone? | |  | |  | |  | | |  | |  |
| 25. | Czy urządzenia (np. tablety, smartfony), i komputery osobiste, na których przetwarzane są dane osobowe, mają włączoną automatyczne blokowanie ekranu po okresie bezczynności użytkownika? | |  | |  | |  | | |  | |  |
| 26. | Czy w Podmiot Przetwarzający stosuje politykę tzw. „czystego biurka”? | |  | |  | |  | | |  | |  |
| 27 | Czy dane osobowe gromadzone w formie papierowej przechowywane są w zamykanych szafach/szufladach bez możliwości dostępu do nich osób nieupoważnionych? | |  | |  | |  | | |  | |  |
| 28. | Czy dokumenty w formie papierowej są niszczone przy pomocy niszczarek dokumentów | |  | |  | |  | | |  | |  |
| 29. | Czy Podmiot Przetwarzający zabezpieczył urządzenia przenośne oraz nośniki pamięci, wynoszone poza obszar przetwarzania kryptograficznie? | |  | |  | |  | | |  | |  |
| 30. | Czy zapewniono mechanizmy umożliwiające szybkie przywrócenie dostępu do danych osobowych oraz przywrócenie systemu w przypadku wystąpienia incydentu fizycznego lub technicznego? | |  | |  | |  | | |  | |  |
| 31. | Czy Podmiot Przetwarzający prowadzi monitorowanie nieudanych prób zalogowania się do systemu oraz blokowanie konta po określonej nieudanej liczbie prób zalogowania? | |  | |  | |  | | |  | |  |
| 32. | Czy zostały wprowadzone mechanizmy kopii zapasowych, czy kopie zapasowe są prowadzone regularnie? | |  | |  | |  | | |  | |  |
| 33. | Czy kopie zapasowe są testowane okresowo pod kątem ich odtworzenia? | |  | |  | |  | | |  | |  |
| 34. | Czy zapewniono oprogramowanie antywirusowe na wszystkich stacjach? | |  | |  | |  | | |  | |  |
| 35. | Czy Podmiot Przetwarzający jest właścicielem infrastruktury fizycznej (serwerownia, serwery) na której funkcjonują systemy IT, w których są przetwarzane dane osobowe? | |  | |  | |  | | |  |  | |
| 36. | Czy Podmiot Przetwarzający wykonywał testy bezpieczeństwa swojego środowiska informatycznego? Jeśli tak, uprzejmie prosimy o udostępnienie wyników. | |  | |  | |  | | |  |  | |
| 37. | Czy w Podmiot Przetwarzający wyznaczył osobę odpowiedzialną za bezpieczeństwo IT? | |  | |  | |  | | |  |  | |
| Jeśli tak, proszę podać służbowe dane kontaktowe tej osoby (imię, nazwisko, nr telefonu, adres e-mail). | |  | | | | | | | |  | |
| 38. | **Czy Podmiot Przetwarzający korzysta chmury publicznej (cloud computing)?** |  | |  | |  | | |  | |  | |
| Jeżeli tak, to z jakiego rozwiązania? |  | | | | | | | | |  | |
| 39. | Czy rozwiązanie chmurowe pozwala na przetwarzanie danych zgodnie z obowiązującymi regulacjami? |  | |  | |  | | |  | |  | |
| 40. | W przypadku stosowania rozwiązań w chmurze, czy stosowane są metody ograniczające dostęp do danych dla osób nieuprawnionych np. szyfrowanie danych? |  | |  | |  | | |  | |  | |
| 41. | Czy systemy IT, w których są przetwarzane dane osobowe zarządzane są przez podmiot zewnętrzny? |  | |  | |  | | |  | |  | |
| 42. | Jeśli administratorem systemu IT lub dostawcą utrzymującym system jest podmiot zewnętrzny, proszę wskazać czy posiada on zdalny dostęp do środowiska IT? |  | |  | |  | | |  | |  | |
| 43. | Czy użytkownicy mają dostęp zdalny do zasobów? Jeśli tak, to w jaki sposób zabezpieczony jest kanał komunikacji? |  | |  | |  | | |  | |  | |
| 44 | Czy Podmiot przetwarzający gwarantuje ciągłość funkcjonowania swojej platformy? |  | |  | |  | | |  | |  | |
| 45 | Czy bezpieczeństwo przetwarzania jest potwierdzane certyfikatami bezpieczeństwa, normami? |  | |  | |  | | |  | |  | |

**\* - wypełnia Administrator Danych**

…………………………………………………………..

Podpis osoby wypełniającej ankietę

|  |  |
| --- | --- |
| **Ocena Podmiotu Przetwarzającego\*** | |
| Kwestie organizacyjne |  |
| Bezpieczeństwo fizyczne |  |
| Bezpieczeństwo środowiska informatycznego |  |
| **Ocena łączna** |  |