…………………………………………………

nazwa podmiotu przetwarzającego

…………………………………………………………………….

imię i nazwisko osoby sporządzającej ankietę dla podmiotu przetwarzającego

|  |  |  |  |
| --- | --- | --- | --- |
| **ANKIETA DLA PODMIOTU PRZETWARZAJĄCEGO** | | | |
| **LP.** | **PYTANIE** | **POZIOM ZGODNOŚCI** | **ODPOWIEDŹ** |
| 1. | Czy zgodnie z art. 29 RODO osoby wykonujące operacje na danych osobowych otrzymały upoważnienia do przetwarzania danych, w których został określony w szczególności zakres przetwarzanych przez te osoby danych? |  |  |
| 2. | Czy osoby upoważnione do przetwarzania danych zobowiązały się do zachowania tajemnicy? |  |  |
| 3. | Czy jesteś w stanie wspomagać ADO przy realizacji praw osób, których dane dotyczą? |  |  |
| 4. | Czy dysponujesz środkami, które pozwalają na usunięcie lub zwrot wszelkich danych osobowych oraz usunięcie ich wszelkich istniejących kopii? |  |  |
| 5. | Czy umożliwisz ADO lub audytorowi upoważnionemu przez ADO przeprowadzania audytów, w tym inspekcji? |  |  |
| 6. | Czy jesteś w stanie informować ADO o naruszeniach ochrony danych osobowych, do których u Ciebie dojdzie? |  |  |
| 7. | Czy stosujesz zatwierdzony kodeks postępowania, o którym mowa w art. 40 RODO? |  |  |
| 8. | Czy posiadasz certyfikat dotyczący wdrożonego systemu zarządzania bezpieczeństwem informacji, zgodnego z wymaganiami normy ISO/IEC 27001 lub innymi adekwatnymi normami? |  |  |
| 9. | Czy posiadasz opracowaną i wdrożoną politykę ochrony danych osobowych lub politykę bezpieczeństwa informacji, bądź inną dokumentację opisującą zasady ochrony danych? |  |  |
| 10. | Czy wyznaczyłeś inspektora ochrony danych lub inną osobę odpowiedzialną za ochronę danych osobowych w Twojej organizacji? |  |  |
| 11. | Czy jesteś w stanie wykazać przestrzeganie ochrony danych m.in. poprzez przedstawienie obowiązujących w Twojej organizacji procedur i dokumentacji dotyczącej ochrony danych osobowych? |  |  |
| 12. | Czy jesteś w stanie zapewnić, aby nowozatrudniony pracownik przed podjęciem czynności związanych z przetwarzaniem danych osobowych został odpowiednio przeszkolony w tym zakresie i zapoznany z obowiązującymi przepisami prawa dotyczącymi ochrony danych oraz z procedurami wdrożonymi w organizacji? |  |  |
| 13. | Czy w ciągu dwóch ostatnich lat Twoja organizacja została poddana zewnętrznej kontroli niezależnych audytorów funkcjonującego systemu ochrony danych? |  |  |
| 14. | Czy korzystasz z usług tylko takich podmiotów zewnętrznych/podwykonawców, którzy zostali przez Ciebie wcześniej sprawdzeni pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych? |  |  |
| 15. | Czy jesteś w stanie zrezygnować ze współpracy z którymś ze swoich podmiotów przetwarzających, jeśli ADO nie wyrazi na nich zgody? |  |  |
| 16. | Czy stosujesz środki kontroli dostępu fizycznego do budynku/budynków tylko dla autoryzowanego personelu? |  |  |
| 17. | Czy dostęp do pomieszczeń pozostających w Twojej dyspozycji po godzinach pracy jest możliwy dla osób trzecich (firma sprzątająca, ochrona). Jeśli „TAK” opisz w „ODPOWIEDZ” czy dostęp ten jest szczegółowo nadzorowany? |  |  |
| 18. | Czy każdy pracownik otrzymuje indywidualny identyfikator do systemów informatycznych? |  |  |
| 19. | Czy masz wdrożone zasady zarządzania hasłami (minimalna długość, złożoność, częstotliwość zmiany itp.)? |  |  |
| 20. | Czy wobec urządzeń mobilnych wynoszonych poza obszar przetwarzania (np. laptopy, dyski) stosujesz zabezpieczenia kryptograficzne? |  |  |
| 21. | Czy pracownicy zostali zobowiązani do zabezpieczenia nieużywanych w danym momencie systemów poprzez blokadę ekranu lub w inny równoważny sposób? |  |  |
| 22. | Czy pracownicy zostali zobowiązani do niezwłocznego odbierania z drukarek wydruków zawierających dane osobowe lub inne poufne informacje? Czy wskazana zasada jest przestrzegana przez pracowników? |  |  |
| 23. | Czy w Twojej organizacji stosowana jest zasada tzw. „czystego biurka”? |  |  |
| 24. | Czy dane osobowe gromadzone w formie papierowej, po godzinach pracy organizacji, przechowywane są w zamykanych szafach/szafkach/szufladach bez możliwości dostępu do nich osób nieupoważnionych? |  |  |
| 25. | Czy zapewniono oprogramowanie antywirusowe na wszystkich stacjach? |  |  |
| 26. | Czy oprogramowanie posiada licencję i jest na bieżąco aktualizowane? |  |  |
| 27. | Czy regularnie sporządzasz kopie zapasowe baz danych? |  |  |
| 28. | Opisz sposób tworzenia kopii zapasowych |  |  |
| 29. | Czy kopie zapasowe przechowywane są w miejscu zapewniającym ich bezpieczeństwo? |  |  |
| 30. | Czy zapewniasz zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie wystąpienia incydentu fizycznego lub technicznego? |  |  |
| 31. | Czy wdrażasz nowe rozwiązania zgodnie z zasadą „privacy by design”? |  |  |
| 32. | Czy prowadzisz rejestr kategorii czynności przetwarzania zawierający wszystkie informacje wskazane w art. 30 ust. 2 RODO? |  |  |
| 33. | Czy posiadasz procedury odtwarzania systemu po awarii oraz ich testowania? |  |  |
| 34. | Czy przetwarzasz dane osobowe (łącznie z kopiami zapasowymi) wyłącznie w krajach Europejskiego Obszaru Gospodarczego? |  |  |

Ilekroć w dokumencie mowa jest o RODO rozumie się przez to Rozporządzeniu 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).

Ilekroć w dokumencie mowa jest o ADO rozumie się przez to Gminę Miejską Starogard Gdański.

**Poziom zgodności:**

**2 – zgodność**

**1 – częściowa zgodność**

**0 - niezgodność**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Data podpis przedstawiciela podmiotu przetwarzającego