**Ankieta oceny spełnienia obowiązków wynikających z przepisów   
o ochronie danych osobowych dla podmiotu przetwarzającego**

**Administrator Danych Osobowych –** Gmina Miasto Elbląg

reprezentowana przez Prezydenta Miasta Elbląg

**Podmiot przetwarzający** – „………………………………………………………

1. **Przedmiot umowy** –

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Lp. | Zagadnienia | TAK | NIE | Uwagi |
| 1 | Czy została wyznaczona osoba odpowiedzialna za monitorowanie przestrzegania przepisów dotyczących ochrony danych osobowych?  np. pracownik podmiotu przetwarzającego, Inspektor Ochrony Danych, firma zewnętrzna. |  |  | …………………………………………………….  /imię i nazwisko, dane kontaktowe/ |
| 2 | Czy została wykonana analiza ryzyka przy przetwarzaniu danych osobowych? |  |  | …………………………………………………….  /data wykonania/aktualizacji analizy ryzyka/ |
| 3 | Czy dane osobowe zostały powierzone do dalszego przetwarzania podwykonawcom? |  |  | W przypadku powierzenia danych do dalszego przetwarzania należy przekazać w Załączniku nr 1 do ankiety listę podwykonawców. |
| 4 | Czy prowadzony jest Rejestr wszystkich kategorii czynności przetwarzania? |  |  | Należy przekazać kopię Rejestru wszystkich kategorii czynności przetwarzania w zakresie przetwarzania powierzonych danych |
| 5 | Czy osoby przetwarzające dane osobowe posiadają upoważnienia do przetwarzania danych osobowych? |  |  | Należy przekazać wzór upoważnienia |
| 6 | Czy prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych? |  |  | …………………………………………………….  /liczba osób upoważnionych/ |
| 7 | Czy osoby przetwarzające dane osobowe zostały zobowiązane do zachowania w tajemnicy informacji dotyczących przetwarzanych danych osobowych oraz sposobie ich zabezpieczenia? |  |  | Należy przekazać wzór oświadczenia  o zachowaniu tajemnicy |
| 8 | Czy osoby przetwarzające dane osobowe zostały zapoznane z przepisami dotyczącymi ochrony danych osobowych? |  |  | …………………………………………………….  /data ostatniego szkolenia/ |
| 9 | Czy zostały opracowane i wdrożone zasady/procedury/instrukcje dotyczące ochrony danych osobowych? |  |  | …………………………….…….……………….  /nazwa dokumentu, data przyjęcia/ |
| 10 | Czy dokumenty w formie papierowej przechowywane są w zamykanych na klucz szafach? |  |  |  |
| 11 | Czy zostały opracowane i wdrożone procedury zarządzania incydentami? |  |  | …………………………….…….……………….  /nazwa dokumentu, data przyjęcia/ |
| 12 | Czy prowadzony jest rejestr naruszeń ochrony danych, w którym dokumentowane są wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia, jego skutki oraz podjęte działania zaradcze? |  |  |  |
| 13 | Czy są wprowadzone zasady nadawania/modyfikacji /odbierania uprawnień w systemach informatycznych? |  |  | …………………………….…….……………….  /nazwa dokumentu, data przyjęcia/ |
| 14 | Czy wprowadzona została zasada czystego biurka? |  |  |  |
| 15 | Czy wprowadzona została zasada czystego monitora? |  |  |  |
| 16 | Czy wprowadzone zostały zasady bezpiecznego uwierzytelnienia użytkownika w systemie informatycznym? |  |  | …………………………….…….……………….  /np. długość i złożoność haseł, częstotliwość zmiany hasła/ |
| 17 | Czy stosowane są mechanizmy automatycznej blokady dostępu do komputera w przypadku dłuższej nieaktywności użytkownika, np. uruchomienie wygaszacza ekranu? |  |  | …………………………….…….……………….  /należy opisać zastosowane mechanizmy/ |
| 18 | Czy systemy informatyczne zabezpieczone są przed szkodliwym oprogramowaniem, takim jak, np. wirusy, konie trojańskie, rootkit? |  |  |  |
| 19 | Czy są stosowane zabezpieczenia na styku z Internetem (np. firewall, antyspam, antywirus)? |  |  |  |
| 20 | Czy została zapewniona odpowiednia ochrona danych osobowych przed utratą ich integralności? |  |  |  |
| 21 | Czy są wykonywane kopie zapasowe i czy są odpowiednio zabezpieczone, np. czy są przechowywane w innym miejscu niż bazy produkcyjne? |  |  | …………………………….…….……………….  /miejsce przechowywania kopii zapasowych/ |
| 22 | Posiadane certyfikaty  (np. ISO/IEC 27001, ISO 31000) |  |  | …………………………….…….……………….  /rodzaj certyfikatu, nazwa firmy akredytacyjnej oraz data ważności certyfikatu/ |
| 23 | W jaki sposób niszczone są dokumenty w formie papierowej? | ………………………………………………….…….………………. | | |
| 24 | W jaki sposób niszczone są elektroniczne nośniki danych (dyski twarde, płyty CD, pendrive)? | ………………………………………………….…….………………. | | |

Podstawa prawna

art. 28 ust. 1 lit. h rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r 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)

............................................................. ……………………………………………………………………………….

Data wypełnienia ankiety podpis i pieczęć osoby upoważnionej