**Data**………………………………………….

**Procesor:** …………………………………………………………………

*(Pełna nazwa podmiotu przetwarzającego)*

|  |
| --- |
| **ankieta DLA podmiotu przetwarzającego** |

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P.** | **PYTANIE** | **TAK/NIE****(+ewentualne wyjaśnienie)** | **WYMÓG** |
| **WIEDZA FACHOWA** |
|  | Czy podmiot przetwarzający posiada wyznaczoną osobę, która wykonuje **zadania dotyczące zapewniania przestrzegania przepisów o ochronie danych osobowych? (Zadanie to może być realizowane także przez podmiot zewnętrzny)** |  |  |
| Czy wyznaczone osoby do wykonywania w/w zadań posiadają odpowiednią wiedzę i przygotowanie praktyczne do wykonywania swoich obowiązków z tego zakresu? |  |  |
|  | Czy dany podmiot przetwarzający wyznaczył inspektora ochrony danych? |  | art. 37 RODO |
|  | Czy podmiot przetwarzający wyznaczył inspektora ochrony danych, mimo że nie wymagają tego przepisy prawa lub też inną osobę/zespół odpowiedzialny za nadzór nad ochroną danych osobowych w organizacji? |  |  |
|  | Czy osoby po stronie **podmiotu przetwarzającego dedykowane do obsługi administratora danych zostały przeszkolone i zapoznane z przepisami o ochronie danych?** |  |  |
|  | Czy osoby zatrudnione w podmiocie przetwarzającym przy przetwarzaniu danych zostały **przeszkolone w zakresie obsługi, w tym bezpiecznego korzystania z systemu informatycznego, jeżeli jest on stosowany do przetwarzania danych przez podmiot przetwarzający?** |  |  |
|  | Czy osoby zatrudnione w podmiocie przetwarzającym przy przetwarzaniu danych zostały **przeszkolone w zakresie zasad bezpieczeństwa informacji?** |  |  |
| **WIARYGODNOŚĆ** |
| 1. | Czy stwierdzono prawomocną decyzją UODO lub innego organu nadzorczego lub prawomocnym wyrokiem sądu naruszenie ochrony danych osobowych przez podmiot przetwarzający? |  |  |
| 2. | Czy podmiot przetwarzający stosuje się do przyjętych przez organ nadzorczy kodeksów podstępowania? |  | art. 40 RODO |
| 3 | Czy podmiot przetwarzający objęty jest monitorowaniem przestrzegania kodeksu postępowania przez akredytowany podmiot monitorujący? |  | art. 41 RODO |
| 4 | Czy podmiot przetwarzający otrzymał certyfikat zgodności z RODO? |  | art.42 RODO |
| **ZASOBY** |
|  | Czy podmiot przetwarzający opracował i wdrożył politykę ochrony danych lub podobną procedurę? Jeśli tak, prosimy o wskazanie daty wdrożenia. |  | art. 24 RODO |
|  | Czy podmiot przetwarzających wdrożył instrukcję postępowania w sytuacji naruszenia ochrony danychosobowych? |  |  |
|  | Czy podmiot przetwarzający prowadzi ewidencję naruszeń przepisów o ochronie danych osobowych, w tym naruszeń bezpieczeństwa danych? |  |  |
|  | Czy podmiot przetwarzający prowadzi rejestry czynności przetwarzania danych osobowych? Jeżeli nie, prosimy o wskazanie powodów. |  | art. 30 RODO |
|  | Czy podmiot przetwarzający wprowadził dokument stanowiący o okresie retencji dokumentów zawierających dane osobowe? |  |  |
|  | Czy podmiot przetwarzający wdrożył zasady zarządzania bezpieczeństwem informacji, w tym: |  |  |
| 1. system zarządzania bezpieczeństwem informacji na podstawie normy ISO 27001? Czy posiada certyfikat?
 |  |  |
| 1. zasady zarządzania bezpieczeństwem informacji z elementami wykorzystania normy ISO 27002?
 |  |  |
| Czy podmiot wdrożył inne zasady ochrony informacji – np. Polityka bezpieczeństwa informacji, itp.? |  |  |
|  | Czy podmiot przetwarzający dobrał zabezpieczenia zapewniające bezpieczeństwo przetwarzanych danych osobowych w odniesieniu do oceny skutków ich przetwarzania dla praw i wolności osób, których dane dotyczą? (na podstawie szacowania ryzyka pod kątem ochrony prywatności - PrivacyImpactAssessment)? |  | Odniesienie do Art. 24, 25, 32 RODO |
|  | Czy szacowanieryzyka zostało udokumentowane, np. czy został stworzony plan postępowania z ryzykiem lub zakres zastosowania (Statement of Applicability)? |  |  |
|  | Czy podmiot przetwarzający okresowo przeprowadza kolejne działania związane z szacowaniem ryzyka pod kątem ochrony prywatności? Czy w przypadku zmiany poziomu ryzyka dobiera nowe środki techniczne i organizacyjne zabezpieczające dane, stosownie do wyników analizy? |  |  |
|  | Czy podmiot przetwarzający wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku związanemu z ich przetwarzaniem, w tym: |  | Art. 32 ust. 1 lit a)-c) RODO |
| a) pseudonimizację i szyfrowanie danych, |  |  |
| b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, |  |  |
| c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego. |  |  |
|  | Czy podmiot przetwarzający prowadzi regularnie audyty dotyczące zasad bezpieczeństwa informacji, w tym danych osobowych, w celu weryfikacji spełniania wymogów polityki ochrony danych lub innej wewnętrznej procedury, w tym ocena skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania? |  | Art. 32 ust. 1 lit d) RODO |
|  | Czy wnioski z audytów zostały udokumentowane, np. w raporcie audytowym? |  |  |
|  | Czy podmiot przetwarzający przeprowadził testy penetracyjne systemów które administruje?  |  |  |
| Czy w ich rezultacie zostały wprowadzone odpowiednie poprawki do systemów informatycznych? |  |  |
|  | Czy podmiot przetwarzający jest przygotowany do poddania się audytowi przeprowadzonemu przez administratora danych lub audytora upoważnionego przez administratora danych? |  |  |
|  | Czy podmiot przetwarzający prowadzi monitoring miejsc szczególnie narażonych na naruszenie ochrony danych osobowych ? |  |  |
|  | Czy osoby delegowane do obsługi administratora posiadają nadane upoważnienia do przetwarzania danych?  |  |  |
| Czy zostało to udokumentowane? |  |  |
|  | Czy osoby upoważnione do przetwarzania danych w ramach obsługi administratora zostały obowiązane do zachowania ich w tajemnicy? |  |  |
|  | Czy podmiot przetwarzający wprowadził procedurę upoważniania osób uczestniczących w przetwarzaniu danych osobowych do ich przetwarzania? |  |  |

 ...........................................................

 *podpis*