|  |  |  |  |
| --- | --- | --- | --- |
| **FORMULARZ OCENY PODMIOTU PRZETWARZAJĄCEGO[[1]](#footnote-1)** | | | |
| Instrukcja wypełniania formularza:   1. Podmiot, wobec którego planowane jest powierzenie przetwarzania danych osobowych / któremu powierzono przetwarzanie danych osobowych w ramach ww. czynności, wypełnia kolumny pn. *Odpowiedź* oraz *Uzasadnienie / Uwagi*. 2. W przypadku wypełniania przez podmiot formularza po powierzeniu mu przetwarzania danych osobowych, treść niektórych pytań, odpowiadających tej sytuacji, zawarto w przypisie. | | | |
| **Lp.** | **PYTANIE** | **ODPOWIEDŹ** *(tak / nie / nie dotyczy)* | **UZASADNIENIE / UWAGI** *(dodatkowe informacje)* |
| **INFORMACJE OGÓLNE** | | | |
| 1. | Czy podmiot przetwarzający powołał w swojej jednostce Inspektora Ochrony danych (IOD) lub inną osobę do wykonywania zadań związanych z ochroną danych osobowych? Jeśli tak, proszę wskazać kiedy. |  |  |
| 2. | Czy podmiotowi, do zrealizowania umowy, która zostanie / została zawarta z administratorem, niezbędne jest przetwarzanie danych osobowych? Należy wskazać w uzasadnieniu / uwagach kategorie danych, których przetwarzanie jest niezbędne do zrealizowania umowy, która zostanie / została zawarta z administratorem/podmiotem przetwarzającym[[2]](#footnote-2). |  |  |
| 3 | Czy podmiot posiada doświadczenie w pełnieniu roli podmiotu, któremu powierzono przetwarzanie danych osobowych? Proszę podać jakie. |  |  |
| 4 | Czy podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania zgodnie z art. 30 ust. 2 RODO? |  |  |
|  | | | |
| 5 | Czy podmiot przetwarzający posiada procedury w obszarze ochrony danych osobowych? Proszę wskazać jakie. Czy te procedury uwzględniają - oprócz zadań administratora - również zadania wynikające z pełnienia roli podmiotu przetwarzającego, o których mowa w art. 28 RODO? |  |  |
| 6 | Czy podmiot przetwarzający stosuje w swojej działalności zasady *privacy by design* oraz *privacy by default*? |  |  |
| 7 | Czy zastosowano środki kontroli dostępu fizycznego w stosunku do budynku lub budynków podmiotu przetwarzającego, gdzie realizowana będzie umowa z administratorem? |  |  |
| 8 | Czy podmiot przetwarzający stosuje odpowiednie zabezpieczenia w systemach informatycznych, w których będą przetwarzane dane osobowe w ramach czynności?  W uzasadnieniu / uwagach należy wskazać, jakie zabezpieczenia są stosowane, lub odwołać się do dokumentów regulujących tę kwestię. |  |  |
| 9 | Czy systemy informatyczne podmiotu przetwarzającego wymuszają okresową zmianę haseł? |  |  |
| 10 | Czy podmiot przetwarzający zapewnił oprogramowanie antywirusowe na komputerach używanych przez jednostkę? |  |  |
| 11 | Czy oprogramowanie, używane w podmiocie przetwarzającym, posiada licencję i jest na bieżąco aktualizowane? |  |  |
| 12 | Czy dyski komputerów przenośnych używane przez podmiot przetwarzający są szyfrowane? |  |  |
| 13 | W jaki sposób są zabezpieczone urządzenia mobilne, używane w podmiocie przetwarzającym? Czy są one zabezpieczone co najmniej hasłem? |  |  |
|  | | | |
| 14 | Czy podmiot przetwarzający zapewnia nowozatrudnionym pracownikom - przed podjęciem przez nich czynności związanych z przetwarzaniem danych osobowych - szkolenie w tym obszarze, w szczególności w zakresie obowiązujących w jednostce procedur wewnętrznych? |  |  |
| 15 | Czy do przetwarzania danych osobowych podmiot przetwarzający dopuszcza jedynie osoby, które otrzymały upoważnienia do dokonywania tej czynności? |  |  |
| 16 | Czy podmiot przetwarzający zobowiązuje pracowników do stosowania obowiązujących w jego jednostce procedur w obszarze ochrony danych osobowych i weryfikuje ich stosowanie? Należy wskazać w uzasadnieniu / uwagach, w jaki sposób potwierdzane jest to zobowiązanie, oraz jak odbywa się weryfikacja jego realizacji. |  |  |
| 17 | Czy pracownicy podmiotu przetwarzającego, którzy przetwarzają dane osobowe, zostali zobowiązani do zachowania ich w tajemnicy / w poufności? |  |  |
| 18 | Czy podmiot przetwarzający weryfikuje, czy pracownicy podmiotu przetwarzającego nie pozostawiają w miejscach ogólnodostępnych wydruków lub dokumentów zawierających dane osobowe? Należy wskazać w uzasadnieniu / uwagach, w jaki sposób odbywa się weryfikacja jego realizacji. |  |  |
| 19 | Czy pracownicy podmiotu przetwarzającego zostali zobowiązani do stosowania zasady tzw. „czystego biurka”? Proszę wskazać czy i w jaki sposób podmiot przetwarzający weryfikuje jej stosowanie w praktyce? |  |  |
| 20 | Czy pracownicy przetwarzający dane osobowe w formie papierowej - po zakończeniu pracy - przechowują je w zamykanych szafach i zabezpieczają je przed dostępem do nich nieuprawnionych osób? |  |  |
|  | | | |
| 21 | Czy podmiot przetwarzający prowadzi rejestr naruszeń ochrony danych osobowych? |  |  |
| 22 | Czy podmiot przetwarzający posiada wdrożone mechanizmy identyfikacji oraz oceny i notyfikacji naruszeń ochrony danych osobowych? Proszę wskazać wdrożone mechanizmy. |  |  |
| 23 | Czy w przypadku incydentu w zakresie danych osobowych zapewniono możliwość szybkiego przywrócenia danych i dostępu do nich? Proszę wskazać wdrożone procedury. |  |  |
| 24 | Czy podmiot przetwarzający dokonał oszacowania ryzyka przetwarzania danych osobowych i czy w jego wyniku konieczne okazało się sporządzenie oceny skutków dla ochrony danych (DPIA)? |  |  |
| 25. | Czy i w jaki sposób podmiot przetwarzający zapewnia realizację praw osób, których dane dotyczą? Czy posiada w tym zakresie ustalone procedury postępowania? Proszę wskazać jakie są to procedury. |  |  |
| 26 | Czy podmiot przetwarzający posiada certyfikaty w zakresie bezpieczeństwa informacji lub wdrożył system zarządzenia bezpieczeństwa informacji? Proszę wskazać jakie. |  |  |
| 27 | Czy podmiot przetwarzający planuje dokonywać transferów powierzonych do przetwarzania danych do państw poza EOG??[[3]](#footnote-3) |  |  |

1. Zgodnie z art. 28 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 4.03.2021, str. 35) jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą [↑](#footnote-ref-1)
2. Ten punkt ma charakter informacyjny, zakres danych powierzonych do przetwarzania określa finalnie Administrator (jeśli zakres będzie inny niż wskazany przez podmiot przetwarzający –odpowiednia adnotacja zostanie zamieszczona w zaleceniach i rekomendacjach ze strony administratora ). W przypadku wypełniania formularza przed podpisaniem umowy powierzenia, zakres danych planowanych do powierzenia powinien być ograniczony do takich danych, które są niezbędne do zrealizowania celu zawieranej umowy .W przypadku wypełniania formularza po zawarciu umowy powierzenia, należy wziąć pod uwagę zakres danych powierzonych do przetwarzania - w uwagach można wskazać, że przetwarzany będzie jedynie ten zakres danych. [↑](#footnote-ref-2)
3. Założeniem Administratora jest nie dokonywanie transferów danych powierzonych do przetwarzania do państw poza EOG. Jeżeli taki transfer miałby następować – należy wskazać mechanizm legalizujący taki transfer. [↑](#footnote-ref-3)