|  |  |  |  |
| --- | --- | --- | --- |
| **Formularz dla podmiotu przetwarzającego dane osobowe w ramach zbioru pn. … na temat posiadanych środków ochrony** | | | |
| Instrukcja wypełniania formularza:   1. Podmiot, wobec którego planowane jest powierzenie przetwarzania danych osobowych / któremu powierzono przetwarzanie danych osobowych w ramach ww. zbioru, wypełnia kolumny pn. *Odpowiedź* oraz *Uwagi*. 2. W przypadku wypełniania przez podmiot formularza po powierzeniu mu przetwarzania danych osobowych, treść niektórych pytań, odpowiadających tej sytuacji, zawarto w przypisie. 3. W części pn. *Ocena zgodności i rekomendacje* administrator danych osobowych może zgłosić podmiotowi, któremu planuje powierzyć przetwarzanie danych osobowych / któremu powierzył przetwarzanie danych osobowych, pewne zalecenia i rekomendacje (bez oficjalnie wiążącego ich charakteru), mające na celu poprawę stopnia bezpieczeństwa przetwarzanych danych poprzez modyfikację stosowanych środków technicznych i organizacyjnych. | | | |
| **lp.** | **PYTANIE** | **ODPOWIEDŹ** (tak / nie / nie dotyczy) | **UWAGI** (dodatkowe informacje) |
| **KWESTIE OGÓLNE** | | | |
| 1. | Czy podmiot przetwarzający powołał w swojej jednostce Inspektora Ochrony danych (IOD) lub inną osobę do wykonywania zadań związanych z ochroną danych osobowych? |  |  |
| 2. | Jakie kategorie danych są niezbędne podmiotowi przetwarzającemu do zrealizowania umowy, która zostanie / została zawarta z administratorem? |  |  |
| 3. | Czy podmiot przetwarzający przetwarza dane osobowe w zakresie, w jakim zostały mu one powierzone przez innych administratorów?[[1]](#footnote-1) |  |  |
| 4. | Czy podmiot przetwarzający prowadzi dla innych administratorów rejestr kategorii czynności przetwarzania zgodnie z art. 30 ust. 2 RODO?[[2]](#footnote-2) |  |  |
| **PROCEDURY** | | | |
| 5. | Czy podmiot przetwarzający posiada procedury w obszarze ochrony danych osobowych? Czy te procedury umożliwiają realizację obowiązków podmiotu przetwarzającego, które wynikają z 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. | Jakiego rodzaju zabezpieczenia w systemach informatycznych, w których będą przetwarzane dane osobowe w ramach zbioru pn. …, stosuje podmiot przetwarzający? |  |  |
| 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? |  |  |
| **PRACOWNICY** | | | |
| 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. | W jaki sposób podmiot przetwarzający zobowiązuje pracowników do stosowania obowiązujących w jego jednostce procedur w obszarze ochrony danych osobowych oraz jak weryfikuje ich stosowanie? |  |  |
| 17. | Czy pracownicy podmiotu przetwarzającego, którzy przetwarzają dane osobowe, zostali zobowiązani do zachowania ich w tajemnicy / w poufności? |  |  |
| 18. | W jaki sposób podmiot przetwarzający weryfikuje, czy pracownicy podmiotu przetwarzającego nie pozostawiają w miejscach ogólnodostępnych wydruków lub dokumentów zawierających dane osobowe? |  |  |
| 19. | Czy pracownicy podmiotu przetwarzającego zostali zobowiązani do stosowania zasady tzw. „czystego biurka”? 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? |  |  |
| **INNE** | | | |
| 21. | Czy w przypadku incydentu w zakresie danych osobowych zapewniono możliwość szybkiego przywrócenia danych i dostępu do nich? |  |  |
| 22. | Czy podmiot przetwarzający dokonał oszacowania ryzyka przetwarzania danych osobowych i czy w jego wyniku konieczne okazało się sporządzenie oceny skutków dla ochrony danych (DPIA)? |  |  |
| 23. | Czy i w jaki sposób podmiot przetwarzający zapewnia realizację praw osób, których dane dotyczą? Czy posiada w tym zakresie ustalone procedury postępowania? |  |  |
| **OCENA ZGODNOŚCI Z RODO PRZEDSTAWIONYCH PRZEZ PODMIOT PRZETWARZAJACY INFORMACJI**  **ORAZ EWENTUALNE ZALECENIA I REKOMENDACJE ZE STRONY ADMINISTRATORA** | | | |
|  | | | |

1. W przypadku wypełniania formularza już po powierzeniu przetwarzania danych osobowych, przedmiotowe pytanie brzmi następująco:

   *Czy podmiot przetwarzający przetwarza dane osobowe w zakresie powierzonym mu przez administratora w ramach zbioru* *pn.… ?* [należy wstawić właściwą nazwę] [↑](#footnote-ref-1)
2. W przypadku wypełniania formularza już po powierzeniu przetwarzania danych osobowych, przedmiotowe pytanie brzmi następująco:

   *Czy w związku z przetwarzaniem danych osobowych w ramach zbioru pn. …* [należy wstawić właściwą nazwę] *podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania zgodnie z art. 30 ust. 2 RODO?* [↑](#footnote-ref-2)