|  |  |  |  |
| --- | --- | --- | --- |
| Ankieta weryfikacyjna podmiotu przetwarzającego | | | |
|  | | | |
|  | | | |
| **Podmiot powierzający** | | Nazwa |  |
| Adres |  |
| NIP |  |
| REGON |  |
| KRS |  |
|  | | | |
| **Podmiot przetwarzający** | | Nazwa |  |
| Adres |  |
| NIP |  |
| REGON |  |
| KRS |  |
|  | | | |
| Data | | |  |
| Imię i nazwisko osoby udzielającej odpowiedzi | | |  |
|  | | | |
| L.p. | PYTANIE | ODPOWIEDŹ  (najlepiej tak/nie) | Uwaga lub uzasadnienie do odpowiedzi |
| **1. ORGANIZACJA** | | | |
| 1.1. | Czy podmiot przetwarzający posiada doświadczenie lub wiedzę, w zakresie świadczenia usług związanych z przetwarzaniem danych osobowych? Jeśli tak, proszę o opis doświadczenia lub przedstawienie dokumentów potwierdzających posiadaną wiedzę. |  |  |
| 1.2. | Czy podmiot przetwarzający musi wyznaczyć IOD? |  |  |
| 1.3. | Czy podmiot przetwarzający wyznaczył IOD? |  |  |
| 1.4. | Czy IOD posiada odpowiedni poziom wiedzy i doświadczenia? Jeśli tak, proszę uzasadnić (najlepiej wskazując posiadane certyfikaty, ukończone studia podyplomowe, udział w szkoleniach itp.) |  |  |
| 1.5. | Czy podmiot przetwarzający posiada dział compliance/security? |  |  |
| 1.6. | Czy w przypadku braku wyznaczenia IOD podmiot przetwarzający posiada specjalistę z zakresu ochrony danych? |  |  |
| 1.7. | Czy specjalista z zakresu ochrony danych posiada odpowiedni poziom wiedzy i doświadczenia? Jeśli tak, proszę uzasadnić (najlepiej wskazać posiadane certyfikaty, ukończone studia podyplomowe, udział w szkoleniach itp.) |  |  |
| 1.8. | Czy IOD oraz specjalista z zakresu ochrony danych posiada odpowiednio wsparcie prawne lub techniczne, w zależności od potrzeb? |  |  |
| 1.9. | Czy podmiot przetwarzający gwarantuje, że IOD posiada zasoby niezbędne do wykonania zadań, a także zasoby niezbędne do utrzymania jego wiedzy fachowej? |  |  |
| 1.10. | Czy członkowie personelu zostali przeszkoleni i zapoznani z przepisami o ochronie danych? Czy jest to udokumentowane? Jeśli tak, proszę wskazać termin ostatniego szkolenia. |  |  |
| 1.11. | Czy członkowie personelu zostali przeszkoleni w zakresie obsługi, w tym bezpiecznego korzystania, z systemów i urządzeń informatycznych? Czy jest to udokumentowane? Jeśli tak, proszę wskazać termin ostatniego szkolenia. |  |  |
| 1.12. | Czy członkowie personelu zostali przeszkoleni w zakresie zasad bezpieczeństwa informacji, w szczególności ochrony danych osobowych? Czy jest to udokumentowane? Jeśli tak, proszę wskazać termin ostatniego szkolenia. |  |  |
| 1.13. | Czy podmiot przetwarzający prowadził kontrolowane ataki socjotechniczne, w tym ataki phishingowe na swój personel? Jeśli tak, to proszę wskazać termin oraz z jakim wynikiem się zakończyły. |  |  |
| 1.14. | Czy podmiot przetwarzający przystąpił i stosuje kodeks postępowania dla swojej branży? Jeśli nie, proszę uzasadnić. |  |  |
| 1.15. | Czy podmiot przetwarzający objęty jest monitorowaniem przestrzegania kodeksu postępowania przez akredytowany podmiot monitorujący? |  |  |
| 1.16. | Czy podmiot przetwarzający posiada certyfikat zgodności z RODO, zgodnie z przepisami rozporządzenia? Jeśli tak, proszę wskazać wystawcę certyfikatu oraz datę uzyskania. |  |  |
| 1.17. | Czy podmiot przetwarzający zamierza korzystać lub korzysta z usług dalszych podmiotów przetwarzających? Jeśli tak, to w jakim zakresie oraz czy dokonał weryfikacji takich podmiotów, w szczególności kiedy ostatnio prowadził u nich audyt bezpieczeństwa, w jakiej formie i jaki był wynik audytu. |  |  |
| 1.18. | Czy podmiot przetwarzający korzysta z usług zewnętrznego podmiotu w zakresie bezpieczeństwa informacji lub zgodności z przepisami RODO np. kancelarie prawne, specjalistyczne firmy IT security itp.? Jeśli tak, to jakiego? |  |  |
| **2. ZABEZPIECZENIA** | | | |
| 2.1. | Czy podmiot przetwarzający prowadzi regularne audyty bezpieczeństwa, w szczególności ochrony danych osobowych? Jeśli tak, to prosimy o wskazanie daty ostatniego audytu oraz wniosków końcowych. |  |  |
| 2.2. | Czy podmiot przetwarzający posiada certyfikaty w zakresie bezpieczeństwa informacji lub wdrożył system zarządzenia bezpieczeństwa informacji? Jeśli tak, proszę wskazać jakie. |  |  |
| 2.3. | Czy, a jeśli tak, to z jakich programów informatycznych (software) korzysta podmiot przetwarzający przy przetwarzaniu powierzonych danych? Czy takie systemy są zabezpieczone adekwatnie do ryzyka? |  |  |
| 2.4. | Czy, a jeśli tak, to z jakich urządzeń informatycznych (hardware) korzysta podmiot przetwarzający przy przetwarzaniu powierzonych danych? Czy takie urządzenia są zabezpieczone adekwatnie do ryzyka? |  |  |
| 2.5. | W jakich lokalizacjach podmiot przetwarzający przetwarza powierzone dane osobowe? Czy te lokalizacje są zabezpieczone adekwatnie do ryzyka? |  |  |
| 2.6. | Czy podmiot przetwarzający korzysta z rozwiązań chmury obliczeniowej? Jeśli tak, to jakiego rodzaju (prywatna/publiczna/hybrydowa) i od jakich dostawców. |  |  |
| 2.7. | Czy podmiot przetwarzający korzysta z systemów informatycznych (software) opartych o model rozwiązań chmury obliczeniowe (SAS)? Jeśli tak, to jakiego rodzaju jest to oprogramowanie. |  |  |
| 2.8. | Czy podmiot przetwarzający będzie przetwarzał powierzone dane osobowe w formie papierowej? Jeśli tak to czy te dokumenty będą zabezpieczone adekwatnie do ryzyka? |  |  |
| 2.9. | Czy podmiot przetwarzający wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku związanemu z ich przetwarzaniem, w tym:  a. pseudonimizację i szyfrowanie danych osobowych?  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?  d. regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania? |  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| **3. INCYDENTY, POSTĘPOWANIA ORGANU, DECYZJE ITP.** | | | |
| 3.1. | Czy u podmiotu przetwarzającego doszło w ciągu ostatnich 12 miesięcy do incydentów bezpieczeństwa? Jeśli tak, to jakiej kategorii i jak często (np. zgubienie pendriva bez danych osobowych raz w roku albo włamanie bez kradzieży danych dwa razy w roku). |  |  |
| 3.2. | Czy u podmiotu przetwarzającego doszło w ciągu ostatnich 12 miesięcy do naruszeń ochrony danych osobowych? Jeśli tak, to jakiej kategorii były to naruszenia, w tym czy podlegały zgłoszeniu do organu nadzorczego (np. zgubienie niezaszyfrowanego laptopa z danymi osobowymi, dwa razy w zeszłym roku, podlegało zgłoszeniu) |  |  |
| 3.3. | Jeśli na pytanie 3.2. odpowiedź brzmiała „tak” to jakie zostały podjęte kroki w celu zaradzenia naruszeniu, w tym przeciwdziałaniu podobnym naruszeniom w przyszłości? |  |  |
| 3.4. | Czy wobec podmiotu przetwarzającego prowadzona była kontrola Prezesa Urzędu Ochrony Danych Osobowych? Jak tak, to kiedy i jaki był jej wynik? |  |  |
| 3.5. | Czy wobec podmiotu przetwarzającego było prowadzone postępowanie Prezesa Urzędu Ochrony Danych Osobowych, na skutek skargi podmiotu danych? Jak tak, to kiedy postępowanie było prowadzone, co było przedmiotem skargi i jaki był wynik postępowania? |  |  |
| 3.6. | Czy podmiot przetwarzający występuje w jakiejkolwiek sprawie sądowej lub sądowo-administracyjnej dot. ochrony danych osobowych? Jeśli tak, to w jakim charakterze, czego dotyczy sprawa oraz jakie jest rozstrzygnięcie? |  |  |
| **4. PRZETWARZANIE TRANSGRANICZNE POZA EOG** | | | |
| 4.1. | Czy podmiot przetwarzający lub dalszy podmiot przetwarzający, z którego usług korzysta podmiot przetwarzający, przetwarza dane osobowe poza EOG? |  |  |
| 4.2. | Jeśli tak, to w jakim kraju? |  |  |
| 4.3. | Jeśli tak, to na jakiej podstawie dane osobowe są transferowane poza EOG? |  |  |
| 4.4. | Jeśli tak, to w jakim celu? |  |  |
| 4.5. | Jeśli tak, to czy jest to związane z rozwiązaniami technicznymi np. korzystanie z serwerów? |  |  |
| 4.6. | Jeśli powierzone dane są przetwarzane na terenie krajów, co do których może zostać utracone prawo do transferu danych to czy podmiot przetwarzający posiada odpowiednią procedurę w celu legalizacji takiego przetwarzania? |  |  |
| **5. POLITYKI I PROCEDURY** | | | |
| 5.1. | Czy podmiot przetwarzający posiada politykę ochrony danych osobowych lub podobną? Jeśli tak, to proszę o potwierdzenie przyjęcia takiej polityki i jej wdrożenia. |  |  |
| 5.2. | Czy podmiot przetwarzający posiada procedury realizacji praw osób, których dane dotyczą oraz spełniania obowiązku informacyjnego? Jeśli tak, to proszę o potwierdzenie przyjęcia takich procedur i ich wdrożenia. |  |  |
| 5.3. | Czy podmiot przetwarzający posiada procedurę postępowania w sprawie naruszenia? Jeśli tak, to proszę o potwierdzenie przyjęcia takie procedury i jej wdrożenia. |  |  |
| 5.4. | Czy podmiot przetwarzający posiada procedurę retencji danych? Jeśli tak, to proszę o potwierdzenie przyjęcia takiej procedury i jej wdrożenia. |  |  |
| 5.5. | Czy podmiot przetwarzający nadaje upoważnienia do przetwarzania danych osobowych personelowi? |  |  |
| 5.6. | Czy podmiot przetwarzający prowadzi rejestr nadanych upoważnień? |  |  |
| 5.7. | Czy podmiot przetwarzający zobowiązuje personel do zachowania w tajemnicy wszelkich danych osobowych? |  |  |
| 5.8. | Czy podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania? |  |  |
| 5.9. | Czy podmiot przetwarzający przeprowadził analizę ryzyka? Jeśli tak, prosimy o załączenie wyników analizy ryzyka dla procesu, który będzie dotyczył powierzonych danych osobowych. |  |  |
| 5.10. | Czy podmiot przetwarzający korzysta z narzędzia wspomagającego zarządzanie bezpieczeństwem danych osobowych? Jeśli tak, to z jakiego. |  |  |