Załącznik nr 7

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **FORMULARZ WERYFIKACYJNY**  **PODMIOTU PRZETWARZAJĄCEGO DLA ADMINISTRATORA** | | | | | |
| 1. Wypełniając Formularz nie poprzestawaj wyłącznie na zaznaczeniu odpowiedniego checkboxa, lecz w miarę możliwości przedstaw dodatkowy, wyczerpujący opis danego zagadnienia. 2. Lista stosowanych przez Twoją organizację środków technicznych i organizacyjnych służących zabezpieczeniu danych osobowych powinna być kompletna i aktualna na dzień wypełnienia Formularza. 3. Prawidłowy oraz kompletny Formularz będzie podstawą dokonania przez Katowicką Specjalną Strefę Ekonomiczną S.A. oceny Twojej organizacji z perspektywy spełnienia wymagań wynikających z przepisów prawa. | | | | | |
| 1. **Gdzie Twoja organizacja ma swoją siedzibę?** | | | | | |
| *(np. „W Europejskim Obszarze Gospodarczym, w Republice Czeskiej”, „Poza Europejskim Obszarem Gospodarczym, w Stanach Zjednoczonych”)* | | | | | |
| 1. **Czy Twoja organizacja będzie przetwarzała powierzone przez nas dane osobowe w jakimkolwiek innym celu niż cel określony w umowie głównej?** | | | | | |
| **TAK** | | | **NIE** | | |
| *Uwagi / dodatkowe informacje…* | | | | | |
| 1. **Czy wyznaczyłeś/aś Inspektora Danych Osobowych? Jeśli nie – kto w Twojej organizacji odpowiada za obszar ochrony danych osobowych?** | | | | | |
| **TAK** | | | **NIE** | | |
| *Uwagi / dodatkowe informacje…* | | | | | |
| 1. **Czy prowadzisz rejestr kategorii czynności przetwarzania zgodnie z wymogami art. 30 ust. 2 RODO? Jeżeli tak – prosimy o jego przesłanie.** | | | | | |
| **TAK** | | | **NIE** | | |
| *Uwagi / dodatkowe informacje…* | | | | | |
| 1. **Czy osoby wykonujące operacje na danych osobowych otrzymują od Ciebie upoważnienia do przetwarzania danych osobowych zgodnie z art. 29 RODO? Jeżeli tak – prosimy o wzór stosowanego upoważnienia.** | | | | | |
| **TAK** | | | **NIE** | | |
| *Uwagi / dodatkowe informacje…* | | | | | |
| 1. **Czy Twoja organizacja gwarantuje, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy?[[1]](#footnote-2) Jeżeli tak – prosimy o wzór stosowanego oświadczenia/zobowiązania.** | | | | | |
| **TAK** | | | **NIE** | | |
| *Uwagi / dodatkowe informacje…* | | | | | |
| 1. **Czy w Twojej organizacji została wdrożona i jest stosowana polityka ochrony danych osobowych?** | | | | | |
| **TAK** | | | **NIE** | | |
| *Uwagi / dodatkowe informacje…* | | | | | |
| 1. **Czy w Twojej organizacji obowiązują procedury postępowania w przypadku naruszenia danych osobowych uwzględniające czas oraz sposób działania?** | | | | | |
| **TAK** | | | **NIE** | | |
| *Uwagi / dodatkowe informacje…* | | | | | |
| 1. **Czy szkolisz oraz zapoznajesz z obowiązującymi zasadami ochrony danych osobowych nowozatrudnionych pracowników/współpracowników? Czy dbasz o odświeżenie tej wiedzy u długotrwałych pracowników/stałych współpracowników poprzez cykliczne szkolenia? Jeżeli tak – prosimy o harmonogram szkoleń odbytych oraz planowanych szkoleń wraz z ich agendą.** | | | | | |
| **TAK** | | | **NIE** | | |
| *Uwagi / dodatkowe informacje…* | | | | | |
| 1. **Czy szkolisz i zapoznajesz z obowiązującymi zasadami ochrony danych osobowych pracowników tymczasowych oraz praktykantów?** | | | | | |
| **TAK** | | | **NIE** | | |
| *Uwagi / dodatkowe informacje…* | | | | | |
| 1. **Czy korzystasz z usług innego podmiotu przetwarzającego (podprocesora) w celu przetwarzania powierzonych mu danych? Jeżeli tak – prosimy o listę aktualnych podprocesorów wraz ze wzorem stosowanej umowy powierzenia.** | | | | | |
| **TAK, korzystam z usług następujących innych podmiotów przetwarzających:** | | | | | **NIE** |
| 1. **Jeśli odpowiedź na pytanie 11. jest twierdząca – czy zweryfikowałeś takie inne podmioty przetwarzające oraz czy zapewniają one, zgodnie z RODO, wymogi w zakresie gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, a jeżeli tak – jakie?** | | | | | |
| **TAK** | | | **NIE** | | |
| *Opis / dodatkowe informacje…* | | | | | |
| 1. **Czy w umowach zawieranych z innymi podmiotami przetwarzającymi (podprocesorami) nakładasz na podprocesorów co najmniej te same obowiązki ochrony danych osobowych jak w umowie powierzenia zawartej z Administratorem (art. 28 ust. 4 RODO)?** | | | | | |
| **TAK** | | | **NIE** | | |
| *Opis / dodatkowe informacje…* | | | | | |
| 1. **Czy będziesz przekazywał lub już przekazujesz dane osobowe do państw trzecich lub organizacji międzynarodowych (np. poza EOG)? Jeśli tak, do jakich? Jakie zabezpieczenie stosujesz w związku z tym?** | | | | | |
| **TAK** | | | **NIE** | | |
| *Opis stosowanych zabezpieczeń / dodatkowe informacje…* | | | | | |
| 1. **Czy w Twojej organizacji przeprowadzony został audyt zgodności z zasadami ochrony danych osobowych przez podmiot zewnętrzny?** | | | | | |
| **TAK** | | | **NIE** | | |
| *Jeżeli tak, prosimy o informację o terminach przeprowadzenia audytów oraz jakie wnioski przedstawiał raport z audytów…* | | | | | |
| 1. **Czy rozwiązania/narzędzia/systemy wykorzystywane przez Twoją organizację umożliwiają eksport wszystkich danych jednego podmiotu danych do powszechnie używanego formatu danych?** | | | | | |
| **TAK** | | | **NIE** | | |
| *Opis działania / dodatkowe informacje…* | | | | | |
| 1. **Czy rozwiązania/narzędzia/systemy umożliwiają eksport danych dotyczących incydentu (informacje obejmujące m.in. określenie ilości rekordów objętych naruszeniem, przyczyny naruszenia). Czy masz możliwość wygenerowania raportu dot. naruszenia?**   **Jeżeli wskazanie konkretnej liczby rekordów objętych naruszeniem nie jest możliwe, prosimy o wskazanie (w polu ,,Dodatkowe informacje”) poziomu dokładności w szacowaniu liczby rekordów oraz opisanie zasad takiego szacowania.** | | | | | |
| **TAK** | | | **NIE** | | |
| *Dodatkowe informacje / wyjaśnienia…* | | | | | |
| 1. **Czy Twoja organizacja zobowiązuje się pokryć wszelkie należności finansowe wynikające z naruszenia zasad ochrony powierzonych mu danych osobowych (w tym pokrycie kar administracyjnych, kar umownych)?**   **W przypadku odpowiedzi ,,NIE” – w polu ,,Dodatkowe informacje” prosimy o wyczerpujące wskazanie ewentualnych ograniczeń oraz ich uzasadnienie.** | | | | | |
| **TAK** | | | **NIE** | | |
| *Dodatkowe informacje / wyjaśnienia…* | | | | | |
| 1. **Czy Twoja organizacja ubezpieczenie na wypadek naruszenia danych osobowych oraz bezpieczeństwa?** | | | | | |
| **TAK** | | | **NIE** | | |
| *Uwagi / dodatkowe informacje…* | | | | | |
| 1. **Jakie z poniższych środków technicznych i organizacyjnych stosuje Twoja organizacja?**   **Poniższa lista stanowi wyłącznie punkt wyjścia – wszystkie dodatkowe/niewymienione w niej środki techniczne i organizacyjne stosowane przez Twoją organizację powinny zostać wskazane i opisane w pkt. 31 formularza.** | | | | | |
| |  |  | | --- | --- | | Tworzenie regularnych automatycznych kopii zapasowych. Prosimy o wskazanie rodzaju kopii zapasowych (całościowe / częściowe), miejsca ich przechowywania i częstotliwości tworzenia oraz częstotliwości testowania skuteczności kopii zapasowych**:**  ……………… | Oprogramowanie antywirusowe komputerów oraz urządzeń mobilnych  Zdalna kontrola dostępu do urządzeń przenośnych | | Pseudonimizacja / szyfrowanie danych | Wymóg łączenia się poprzez VPN | | Posiadanie aktualnych licencji programów i systemów komputerowych | Cykliczne testy penetracyjne | | Zabezpieczenie sprzętów przenośnych (np. wymóg wprowadzenia hasła, możliwość zdalnego blokowania dostępu) | Indywidualne identyfikatory w systemach informatycznych | | System IDS / IPS | Możliwość odtworzenia danych po wystąpieniu awarii systemów | | Całodobowa ochrona budynku | Polityka haseł (np. wymogi stopnia trudności hasła / cyklicznie zmiany) | | System alarmowy / antywłamaniowy | Antywłamaniowe drzwi i okna | | Możliwość sprawdzenia logów systemowych | Obowiązek blokady ekranu w razie odejścia od stanowiska / komputera | | Przechowywanie danych w formie papierowej w zabezpieczonych szafkach / pomieszczeniach | Gradacja dostępu do danych | | Monitoring wizyjny  Kontrola pomieszczeń / nadzór nad dostępem osób trzecich (np. firmy sprzątającej) | Inne rodzaje monitoringu.Prosimy o ich wskazanie**:**  **………………** | | Polityka „czystego biurka” | Działania w myśl zasady *privacy by default* | | Wdrażanie nowych rozwiązań zgodnie z zasadą *privacy by design* | Przeprowadzenie oceny skutków dla ochrony danych**.** Prosimy o wskazanie, dla jakich operacji ocena została przeprowadzona**:**  **………………** | | Stosowanie bezpiecznych kopert / pojemników transportowych **/** innych środków zabezpieczających transport danych osobowych | Cykliczne audyty, w tym audyty bezpieczeństwa IT / cyberbezpieczeństwa | | Szyfrowanie pamięci urządzeń przenośnych / zewnętrznych nośników pamięci | Usuwanie / utylizacja danych osobowych lub nośników pamięci oraz ich kopii uniemożliwiająca powrotne odtworzenie danych osobowych | | Wdrożenie SZBI | Zapewnienie zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania. | | Procedura reagowania na incydenty | Gotowość do reagowania na żądanie osoby, której dane dotyczą w zakresie realizacji jej praw | | Testy socjotechniczne | Regularna aktualizacja systemów operacyjnych | | Zabezpieczenie dostępu do serwerowni | Serwery proxy i bramki filtrujące | | Zarządzanie pojemnością systemów | Zapasowe centrum danych | | Umowy serwisowe | Lokalizacja infrastruktury informatycznej w lokalizacjach bezpiecznych | | | | | | |
| 1. **Czy w Twojej organizacji obowiązują procedury realizacji praw podmiotów danych (żądanie dostępu do informacji/organiczenia przetwarzania/usunięcia/przenoszenia danych)?** | | | | | |
| **TAK** | | **NIE** | | | |
| *Uwagi / dodatkowe informacje…* | | | | | |
| 1. **Czy stosowany w Twojej organizacji system zabezpieczeń odnosi się do wszystkich operacji, serwisów oraz systemów, w ramach których dochodzi do czynności związanych z przetwarzaniem informacji poufnych?** | | | | | |
| **TAK** | | | **NIE** | | |
| *Uwagi / dodatkowe informacje…* | | | | | |
| 1. **W jaki sposób przechowujesz dane osobowe powierzone przez Administratora oraz w jaki sposób dane osobowe powierzone przez Administratora są separowane od danych powierzonych przez inne podmioty korzystające z usług Twojej organizacji?** | | | | | |
| *Informacje / wyjaśnienia…* | | | | | |
| 1. **Czy dokonujesz przeglądy i aktualizacje stosowanych środków technicznych i organizacyjnych, a jeżeli tak – z jaką częstotliwością?** | | | | | |
| **TAK** | | | **NIE** | | |
| *Dodatkowe informacje / wyjaśnienia…* | | | | | |
| 1. **Jak często dokonujesz rewizji ustalonych procedur bezpieczeństwa i prywatności?** | | | | | |
| **NATYCHMIAST W PRZYPADKU NASTĄPIENIA ISTOTNYCH ZMIAN.** | **KILKA RAZY W ROKU.** | | **RAZ W ROKU.** | **RZADZIEJ NIŻ RAZ W ROKU.** | |
| *Uwagi / dodatkowe informacje…* | | | | | |
| 1. **Jakie zasoby wykorzystujesz w związku z przetwarzaniem danych osobowych powierzonych przez Administratora?** | | | | | |
| *Informacje / wyjaśnienia…* | | | | | |
| 1. **Jakie certyfikaty, zaświadczenia, normy lub mechanizmy funkcjonują w Twojej organizacji, które potwierdzają wiedzę fachową z zakresu ochrony danych osobowych, w tym w szczególności w zakresie bezpieczeństwa informacji/danych osobowych?** | | | | | |
| *Informacje / wyjaśnienia…* | | | | | |
| 1. **Czy przeprowadziłeś analizę ryzyka lub ocenę skutków dla ochrony danych (DPIA) w zakresie przetwarzania danych osobowych powierzonych przez Spółkę? Jeżeli tak – prosimy o przesłanie wniosków z przeprowadzonych analiz/ocen.** | | | | | |
| *Informacje / wyjaśnienia…* | | | | | |
| 1. **Dalsze informacje/jakie inne środki techniczne i organizacyjne stosuje Twoja organizacja? Jakie standardy lub normy (o ile mają zastosowanie) stosujesz[[2]](#footnote-3)?** | | | | | |
| *(np. norma PN-EN ISO/IEC 27001:2017-06, zgłaszanie naruszeń ochrony danych osobowych do Administratora w 24 godziny, system antywirusowy od dostawcy X, polityka haseł Podmiotu Przetwarzającego polega na cyklicznej zmianie hasła przez pracowników Podmiotu Przetwarzającego co 30 dni)*  *(Prosimy o wskazanie w tym miejscu wszelkich uwag do odpowiedzi z punktu 22 Formularza).* | | | | | |

1. Artykuł 28 ust. 3 lit. b RODO. [↑](#footnote-ref-2)
2. *W szczególności uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, Podmiot Przetwarzający wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku: (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.* [↑](#footnote-ref-3)