## LISTA KONTROLNA DLA POTENCJALNYCH PODMIOTÓW PRZETWARZAJĄCYCH

DOTYCZĄCA STOPNIA SPEŁNIENIA WYMAGAŃ TECHNICZNYCH I ORGANIZACYJNYCH WOBEC PODMIOTÓW, KTÓRYM POWIERZA SIĘ PRZETWARZANIE DANYCH OSOBOWYCH

Szanowni Państwo!

Zwracamy się z prośbą o wypełnienie niniejszej listy kontrolnej, która pozwoli nam ocenić czy Państwa firma zapewnia wystarczającą gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, dzięki którym przetwarzanie danych osobowych będzie zgodne z przepisami RODO i będzie chroniło prawa osób, których dotyczą dane.
Jednocześnie informujemy, że dane przekazane nam przez Państwa będą dostępne wyłącznie dla osób upoważnionych. Informacje przekazane przez Państwa są traktowane jako poufne i nie będą udostępniane osobom trzecim.

| **Dane firmy** | |
|---|---|
| Nazwa Firmy: | |
| Adres: | |
| **Wypełniający ankietę** | |
| Imię i Nazwisko: | |
| Stanowisko: | |
| Data wypełnienia: | |

| Lp. | PYTANIE | TAK / NIE/ NIE DOTYCZY | UWAGI |
|---|---|---|---|
| 1 | Czy przeprowadzają Państwo udokumentowaną analizę ryzyka i uwzględniają w niej ryzyka wynikające z przypadkowego lub niezgodnego z prawem:<br>- zniszczenia,<br>- utraty,<br>- modyfikacji,<br>- nieuprawnionego ujawnienia lub dostępu do danych? | TAK | |
| 2 | Czy w związku z przetwarzaniem danych na zlecenie Administratora (POSiR) zidentyfikowali Państwo zagrożenie/a mogące z dużym prawdopodobieństwem skutkować wysokim ryzykiem naruszenia praw lub wolności osób fizycznych?<br>Jeżeli tak należy dokładnie je opisać w polu Uwagi. | NIE | |
| 3 | Czy wdrożyli Państwo odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający zidentyfikowanym przez Państwa ryzykom zgodnie z art. 32 RODO? | TAK | |
| 4 | Jakie środki techniczne stosują Państwo w celu zapewnienia odpowiedniego poziomu bezpieczeństwa dla ochrony danych? - proszę wybrać (postawić znak X) w polu Uwagi lub wpisać inne przez Państwa stosowane. | | [ x ] pomieszczenia zabezpieczone drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi)<br><br>[ ] pomieszczenia zabezpieczone drzwiami o podwyższonej odporności ogniowej >= 30 min<br><br>[ ] pomieszczenia zabezpieczone drzwiami o podwyższonej |

| | | | |
|---|---|---|---|
| | Mamy świadomość, że każda z firm dobierając zabezpieczenia uwzględnia stan wiedzy technicznej, koszt ich wdrażania, ryzyko naruszenia praw lub wolności osób fizycznych oraz charakter, zakres, kontekst i cele przetwarzania danych osobowych. Dlatego też **nie wymagamy wdrożenia wszystkich zabezpieczeń** uwzględnionych w polu Uwagi. | | odporności na włamanie – drzwi klasy C<br><br>[ ] okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej<br><br>[ ] pomieszczenia, w których przetwarzane są dane wyposażone są w system alarmowy/przeciwwłamaniowy<br><br>[ ] dostęp do pomieszczeń objęty jest systemem kontroli dostępu<br><br>[ ] dostęp do pomieszczeń kontrolowany jest przez system monitoringu wizyjnego<br><br>[ ] dostęp do pomieszczeń jest w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony<br><br>[ ] dostęp do pomieszczeń przez całą dobę jest nadzorowany przez służbę ochrony<br><br>[ x ] pracownicy posiadają dostęp jedynie do pomieszczeń, do których jest to niezbędne ze względu na realizowane obowiązki<br><br>[ x ] dane w formie papierowej przechowywane są w zamkniętej, szafie lub sejfie, kopie zapasowe/archiwalne danych osobowych przechowywane są w zamkniętej szafie lub sejfie,<br><br>[ x ] pomieszczenia, w których przetwarzane są dane są zabezpieczone przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy<br><br>[ x ] dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów<br><br>[ ] zastosowano urządzenia typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania<br><br>[ x ] dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła<br><br>[ ] dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem karty procesorowej oraz kodu PIN lub tokena<br><br>[ x ] zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity<br><br>[ ] użyto systemu Firewall do ochrony dostępu do sieci komputerowej<br><br>[ ] wykorzystano środki pozwalające na rejestrację zmian |

| | | | |
|---|---|---|---|
| | | | wykonywanych na poszczególnych elementach zbioru danych osobowych w systemie informatycznym (logi)<br><br>[ ] zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego w systemie informatycznym zbioru danych osobowych<br><br>[ x ] dostęp do danych osobowych w systemie informatycznym wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (oprócz hasła do systemu operacyjnego)<br><br>[ x ] zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do systemu służącego do przetwarzania danych<br><br>[ x ] systemy wymuszają jakość haseł użytkowników (różne grupy znaków, długość haseł)<br><br>[ x ] zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika<br><br>[ ] zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji<br><br>[ ] dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia<br><br>[ x ] firma korzysta z systemów operacyjnych, które mają aktualne wsparcie producenta<br><br>[ ] firma monitoruje w aktywny sposób działanie serwerów, ruch na serwerach, nieautoryzowane próby wejścia na serwer, próby złamania zabezpieczeń<br><br>[ ] firma prowadzi dziennik administracyjny systemu i prowadzi w nim ewidencję zdarzeń i czynności administracyjnych<br><br>[ ] firma wykonuje kopie zapasowe danych i konfiguracji systemów teleinformatycznych oraz weryfikuje regularnie możliwość ich odtworzenia<br><br>[ ] firma przechowuje kopie zapasowe systemów w innej lokalizacji niż dane produkcyjne<br><br>[ ] w firmie przeprowadzane są testy penetracyjne/audyty bezpieczeństwa systemów teleinformatycznych<br><br>[ ] w przypadku pracy zdalnej wykorzystuje się bezpieczne kanały komunikacji – VPN<br><br>[ ] w firmie nadzoruje się wykorzystywanie pamięci USB<br><br>[ x ] w firmie zabronione jest wykorzystanie nieautoryzowanych nośników USB<br><br>[ ] INNE – proszę wpisać jakie<br>..... |

| | | | |
|---|---|---|---|
| | | | ..... <br> ..... |
| 5 | Jakie środki organizacyjne stosują Państwo w celu zapewnienia odpowiedniego poziomu bezpieczeństwa dla ochrony danych? - proszę wybrać (postawić znak X) w polu Uwagi lub wpisać inne przez Państwa stosowane.<br><br>Mamy świadomość, że każda z firm dobierając zabezpieczenia uwzględnia stan wiedzy technicznej, koszt ich wdrażania, ryzyko naruszenia praw lub wolności osób fizycznych oraz charakter, zakres, kontekst i cele przetwarzania danych osobowych. Dlatego też **nie wymagamy wdrożenia wszystkich zabezpieczeń** uwzględnionych w polu Uwagi. | | [ x ] w firmie jest wdrożona niezbędna dokumentacja w obszarze bezpieczeństwa informacji i ochrony danych osobowych zgodnie z mającymi zastosowanie regulacjami prawnymi (polityki, procedury, instrukcje itp.) - wpisać jakie: Polityka bezpieczeństwa<br><br>[ ] firma posiada certyfikowany system zarządzania bezpieczeństwem informacji zgodny z ISO/IEC 27001<br><br>[ x ] prowadzona jest ewidencja osób upoważnionych do przetwarzania danych<br><br>[ ] prowadzone są regularnie audyty dotyczące zasad bezpieczeństwa informacji, w tym danych osobowych<br><br>[ ] INNE – proszę wpisać jakie<br>.....<br>.....<br>..... |
| 6 | Czy posiadają Państwo zdolność do ciągłego zapewniania poufności, integralności, dostępności i odporności systemów i usług przetwarzania powierzonych danych? | TAK | |
| 7 | Czy posiadają Państwo zdolność do szybkiego przywrócenia dostępności danych w razie incydentu? | TAK | |
| 8 | Czy prowadzą Państwo regularne testowanie, mierzenie i ocenianie skuteczności zastosowanych zabezpieczeń? | TAK | |
| 9 | Czy Państwa pracownicy, którzy będą przetwarzać powierzone dane mają wydane upoważnienia do przetwarzania danych osobowych? | TAK | |
| 10 | Czy osoby upoważnione do przetwarzania danych zobowiązały się do zachowania tajemnicy? | TAK | |
| 11 | Czy osoby upoważnione do przetwarzania danych zostały odpowiednio przeszkolone w zakresie ochrony danych osobowych? | TAK | |
| 12 | Czy są Państwo w stanie wspomagać administratora poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw? | TAK | |
| 13 | Czy są Państwo w stanie wspomagać administratora w wywiązywaniu się z obowiązków związanych z zabezpieczaniem danych określonych w art. 32-36 RODO? | TAK | |

| | | | |
|---|---|---|---|
| 14 | Czy dysponują Państwo środkami, które pozwalają na usunięcie lub zwrot wszelkich danych osobowych oraz usunięcie ich wszelkich istniejących kopii? | TAK | |
| 15 | Czy zamierzają Państwo przy przetwarzaniu powierzonych przez nas danych osobowych korzystać z podprocesora (podwykonawcy)? Jeżeli tak proszę w polu Uwagi wskazać jakiego/jakich i w jakim zakresie. | TAK | Hosting poczty elektronicznej |
| 16 | Jeżeli korzystają Państwo z podprocesora, czy ocenili Państwo, że zapewnia on wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych zgodnie z art. 28 ust. 1 RODO? | TAK | |
| 17 | Jeżeli korzystają Państwo z podprocesora, czy mają Państwo podpisaną z nim umowę powierzenia danych osobowych? | TAK | |
| 18 | Czy są Państwo w stanie zrezygnować ze współpracy z którymś ze swoich podmiotów przetwarzających, jeśli administrator danych nie wyrazi na nich zgody? | TAK | |
| 19 | Czy umożliwią Państwo administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji? | TAK | |
| 20 | Czy potrafią Państwo prawidłowo identyfikować naruszenia ochrony danych osobowych zgodnie z art. 33 RODO? | TAK | |
| 21 | Czy Państwa pracownicy są świadomi spoczywającej na nich odpowiedzialności dotyczącej możliwie najszybszego zgłaszania zdarzeń związanych z bezpieczeństwem informacji, w tym danych osobowych? | TAK | |
| 22 | Czy Państwa pracownicy posiadają wiedzę komu w Państwa firmie powinni zgłaszać incydenty bezpieczeństwem informacji, w tym danych osobowych? | TAK | |
| 23 | Czy są Państwo w stanie informować administratora o naruszeniach ochrony danych osobowych, do których u Państwa dojdzie w ciągu 24 godzin od stwierdzenia naruszenia? | TAK | |
| 24 | Czy posiadają Państwo wiedzę na temat prowadzenia rejestru kategorii czynności przetwarzania zgodnie z art. 30 RODO? | TAK | |
| 25 | Czy wyznaczyli Państwo inspektora | NIE | |

| | | | |
|---|---|---|---|
| | ochrony danych?<br>Jeżeli tak, w polu uwagi należy wpisać imię i nazwisko, nr telefonu oraz adres e-mail. | | |
| 26 | Czy jesteście Państwo gotowi podpisać umowę powierzenia przygotowaną przez POSiR? | TAK | |
| 27 | Czy przekazujecie Państwo powierzone dane do państwa trzeciego? Jeżeli tak - w oparciu o jaką podstawę prawną? (pole Uwagi) | NIE | |