

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 gwarancję 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: - zniszczenia, - utraty, - modyfikacji, - nieuprawnionego ujawnienia lub dostępu do danych?		
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? Jeżeli tak należy dokładnie je opisać w polu Uwagi.		
3	Czy wdrożyli Państwo odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający zidentyfikowanym przez Państwa ryzykom zgodnie z art. 32 RODO?		
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		<input type="checkbox"/> pomieszczenia zabezpieczone drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi) <input type="checkbox"/> pomieszczenia zabezpieczone drzwiami o podwyższonej odporności ogniowej >= 30 min

<p>Państwa stosowane.</p> <p>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.</p>	<p><input type="checkbox"/> pomieszczenia zabezpieczone drzwiami o podwyższonej odporności na włamanie – drzwi klasy C</p> <p><input type="checkbox"/> okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej</p> <p><input type="checkbox"/> pomieszczenia, w których przetwarzane są dane wyposażone są w system alarmowy/przeciwwłamaniowy</p> <p><input type="checkbox"/> dostęp do pomieszczeń objęty jest systemem kontroli dostępu</p> <p><input type="checkbox"/> dostęp do pomieszczeń kontrolowany jest przez system monitoringu wizyjnego</p> <p><input type="checkbox"/> dostęp do pomieszczeń jest w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony</p> <p><input type="checkbox"/> dostęp do pomieszczeń przez całą dobę jest nadzorowany przez służbę ochrony</p> <p><input type="checkbox"/> pracownicy posiadają dostęp jedynie do pomieszczeń, do których jest to niezbędne ze względu na realizowane obowiązki</p> <p><input type="checkbox"/> dane w formie papierowej przechowywane są w zamkniętej, szafie lub sejfie, kopie zapasowe/archiwalne danych osobowych przechowywane są w zamkniętej szafie lub sejfie,</p> <p><input type="checkbox"/> pomieszczenia, w których przetwarzane są dane są zabezpieczone przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy</p> <p><input type="checkbox"/> dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów</p> <p><input type="checkbox"/> zastosowano urządzenia typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania</p> <p><input type="checkbox"/> dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła</p> <p><input type="checkbox"/> 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</p> <p><input type="checkbox"/> zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity</p> <p><input type="checkbox"/> użyto systemu Firewall do ochrony dostępu do sieci komputerowej</p> <p><input type="checkbox"/> wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych w systemie informatycznym (logi)</p> <p><input type="checkbox"/> zastosowano środki umożliwiające określenie praw dostępu do</p>
---	--

		<p>wskazanego zakresu danych w ramach przetwarzanego w systemie informatycznym zbioru danych osobowych</p> <p><input type="checkbox"/> dostęp do danych osobowych w systemie informatycznym wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (oprócz hasła do systemu operacyjnego)</p> <p><input type="checkbox"/> zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do systemu służącego do przetwarzania danych</p> <p><input type="checkbox"/> systemy wymuszają jakość haseł użytkowników (różne grupy znaków, długość haseł)</p> <p><input type="checkbox"/> zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika</p> <p><input type="checkbox"/> zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji</p> <p><input type="checkbox"/> dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia</p> <p><input type="checkbox"/> firma korzysta z systemów operacyjnych, które mają aktualne wsparcie producenta</p> <p><input type="checkbox"/> firma monitoruje w aktywny sposób działanie serwerów, ruch na serwerach, nieautoryzowane próby wejścia na serwer, próby złamania zabezpieczeń</p> <p><input type="checkbox"/> firma prowadzi dziennik administracyjny systemu i prowadzi w nim ewidencję zdarzeń i czynności administracyjnych</p> <p><input type="checkbox"/> firma wykonuje kopie zapasowe danych i konfiguracji systemów teleinformatycznych oraz weryfikuje regularnie możliwość ich odtworzenia</p> <p><input type="checkbox"/> firma przechowuje kopie zapasowe systemów w innej lokalizacji niż dane produkcyjne</p> <p><input type="checkbox"/> w firmie przeprowadzane są testy penetracyjne/audyty bezpieczeństwa systemów teleinformatycznych</p> <p><input type="checkbox"/> w przypadku pracy zdalnej wykorzystuje się bezpieczne kanały komunikacji – VPN</p> <p><input type="checkbox"/> w firmie nadzoruje się wykorzystywanie pamięci USB</p> <p><input type="checkbox"/> w firmie zabronione jest wykorzystanie nieautoryzowanych nośników USB</p> <p><input type="checkbox"/> INNE – proszę wpisać jakie </p>
5	Jakie środki organizacyjne stosują Państwo w celu zapewnienia odpowiedniego poziomu	<p><input type="checkbox"/> w firmie jest wdrożona niezbędna dokumentacja w obszarze bezpieczeństwa informacji i ochrony danych osobowych zgodnie z mającymi zastosowanie regulacjami prawnymi (polityki, procedury,</p>

	<p>bezpieczeństwa dla ochrony danych? - proszę wybrać (postawić znak X) w polu Uwagi lub wpisać inne przez Państwa stosowane.</p> <p>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.</p>	<p>instrukcje itp.) - wpisać jakie</p> <p>.....</p> <p>[] firma posiada certyfikowany system zarządzania bezpieczeństwem informacji zgodny z ISO/IEC 27001</p> <p>[] prowadzona jest ewidencja osób upoważnionych do przetwarzania danych</p> <p>[] prowadzone są regularnie audyty dotyczące zasad bezpieczeństwa informacji, w tym danych osobowych</p> <p>[] INNE – proszę wpisać jakie</p> <p>.....</p> <p>.....</p>
6	Czy posiadają Państwo zdolność do ciągłego zapewniania poufności, integralności, dostępności i odporności systemów i usług przetwarzania powierzonych danych?	
7	Czy posiadają Państwo zdolność do szybkiego przywrócenia dostępności danych w razie incydentu?	
8	Czy prowadzą Państwo regularne testowanie, mierzenie i ocenianie skuteczności zastosowanych zabezpieczeń?	
9	Czy Państwa pracownicy, którzy będą przetwarzać powierzone dane mają wydane upoważnienia do przetwarzania danych osobowych?	
10	Czy osoby upoważnione do przetwarzania danych zobowiązały się do zachowania tajemnicy?	
11	Czy osoby upoważnione do przetwarzania danych zostały odpowiednio przeszkolone w zakresie ochrony danych osobowych?	
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?	
13	Czy są Państwo w stanie wspomagać administratora w wywiązywaniu się z obowiązków związanych z zabezpieczaniem danych określonych w art. 32-36 RODO?	
14	Czy dysponują Państwo środkami, które pozwalają na usunięcie lub zwrot wszelkich danych osobowych oraz usunięcie ich wszelkich istniejących	

	kopii?		
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.		
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?		
17	Jeżeli korzystają Państwo z podprocesora, czy mają Państwo podpisaną z nim umowę powierzenia danych osobowych?		
18	Czy są Państwo w stanie zrezygnować ze współpracy z któryms z swoich podmiotów przetwarzających, jeśli administrator danych nie wyrazi na nich zgody?		
19	Czy umożliwią Państwo administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji?		
20	Czy potrafią Państwo prawidłowo identyfikować naruszenia ochrony danych osobowych zgodnie z art. 33 RODO?		
21	Czy Państwa pracownicy są świadomi spoczywającej na nich odpowiedzialności dotyczącej możliwie najszybszego zgłaszania zdarzeń związanych z bezpieczeństwem informacji, w tym danych osobowych?		
22	Czy Państwa pracownicy posiadają wiedzę komu w Państwa firmie powinni zgłaszać incydenty bezpieczeństwem informacji, w tym danych osobowych?		
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?		
24	Czy posiadają Państwo wiedzę na temat prowadzenia rejestru kategorii czynności przetwarzania zgodnie z art. 30 RODO?		
25	Czy wyznaczyli Państwo inspektora ochrony danych?		
26	Czy jesteście Państwo gotowi podpisać umowę powierzenia przygotowaną przez POSiR?		

27	Czy przekazujecie Państwo powierzone dane do państwa trzeciego? Jeżeli tak - w oparciu o jaką podstawę prawną? (pole Uwagi)		
----	--	--	--