**Lista kontrolna podmiotu przetwarzającego**

Na podstawie umowy powierzenia przetwarzania danych, których administratorami są **Burmistrz Gminy Żukowo, Rada Miejska, Przewodniczący Rady Miejskiej, Kierownik USC i Gmina Żukowo** oraz w związku z art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO) podmiot przetwarzający jest zobowiązany do umożliwienia przeprowadzania audytów przez Administratora (dalej jako ADO).

Niniejsza lista kontrolna ma na celu wykazanie przestrzegania przepisów RODO oraz podnoszenie świadomości w zakresie ochrony powierzonych danych osobowych. Poniższe pytania nie dotyczą zabezpieczeń stosowanych wobec wszystkich danych, będących w posiadaniu podmiotu, ale jedynie wobec danych powierzonych.

|  |  |
| --- | --- |
| **Nazwa i siedziba podmiotu przetwarzającego** |  |
| **Data wypełnienia listy kontrolnej** |  |
| **Osoba odpowiedzialna** |  |
| **Osoba/Osoby wypełniająca** |  |

UWAGA: Odpowiedź „Nie” lub „nie dotyczy” wymaga krótkiego wyjaśnienia.

|  |  |
| --- | --- |
| Środki organizacyjne | |
|  | Czy powołano Inspektora Ochrony Danych lub wyznaczono pracownika do pełnienia zadań związanych z ochroną danych osobowych?  *- należy przesłać skan dokumentu wyznaczającego IOD*  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy opracowano i wdrożono dokumentację ochrony danych opisującą zasady przetwarzania i zabezpieczania danych osobowych (np. polityka ochrony danych)?  *- należy przesłać skan dokumentu wdrażającego – Zarządzenie, oficjalna informacja itp.*  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy prowadzony jest rejestr kategorii czynności przetwarzania zwierający wszystkie informacje wskazane w art. 30 ust. 2 RODO?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy osoby biorące udział w przetwarzaniu powierzonych danych osobowych zostały upoważnione do przetwarzania danych?  *- przy projektach europejskich należy przesłać skan wzoru upoważnienia do przetwarzania danych osobowych.*  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy pracownicy dopuszczeni do pracy z danymi powierzonymi zostali zobowiązani do zachowania tajemnicy lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy pracownicy dopuszczeni do pracy z danymi powierzonymi zostali przeszkoleni z zakresu ochrony danych powierzonych i uświadomieni w zakresie ochrony danych osobowych dotyczących danych powierzonych?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy stworzono procedurę przechowywania/archiwizowania dokumentacji, która zawiera powierzone dane osobowe?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy organizacja posiada procedury szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy zostały wdrożone procedury, umożliwiające skuteczne zgłoszenie naruszenia bezpieczeństwa powierzonych danych osobowych?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
| Podpowierzenie | |
|  | Czy w procesie przetwarzania powierzonych danych wykorzystywane są usługi innych podwykonawców (tzw. podpowierzenie przetwarzania danych)?  *- jeżeli tak, należy przesłać zestawienie zawierające: nazwę podmiotu, zakres działań, datę od kiedy dane osobowe są powierzone.*  *- jeżeli nie, w pkt od 12 do 14 należy zaznaczyć: NIE DOTYCZY.*  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy z podmiotami, o których mowa w pkt 10 zostały podpisane umowy/porozumienia/inny instrument prawny regulujący podpowierzenie zgodne z art. 28 ust. 3 RODO?  *- jeżeli TAK należy załączyć skan umowy (bez kwot i innych danych stanowiących tajemnicę przedsiębiorstwa)*  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy podmioty zewnętrzne, o których mowa w pkt 10 zostały sprawdzone pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych, o których mowa w art. 32 RODO w związku z art. 28 ust. 4 RODO?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy przed podpisaniem umowy z podmiotami, o których mowa w pkt 10, uzyskano zgodę Administratora?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
| Zabezpieczenia fizyczne | |
|  | Czy zastosowano środki kontroli dostępu fizycznego do budynku/budynków tylko dla autoryzowanego personelu w miejscu przechowywania powierzonych danych?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy dostęp do pomieszczeń pozostających w dyspozycji podmiotu przetwarzającego po godzinach pracy jest możliwy dla osób trzecich (m.in. firma sprzątająca, ochrona)?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy powierzone dane osobowe gromadzone w formie papierowej, po godzinach pracy organizacji, przechowywane są w zamykanych szafach/szafkach/szufladach bez możliwości dostępu do nich osób nieupoważnionych (tzw. zasada „czystego biurka”)?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy pracownicy zostali zobowiązani do niszczenia dokumentów zawierających dane osobowe przy użyciu niszczarek, które nie pozwalają na odtworzenie dokumentu w łatwy sposób?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Proszę zaznaczyć **zastosowane** elementy zabezpieczenia fizycznego:  pomieszczenia zamykane na klucz;  klucze do pomieszczeń zdawane na portierni, recepcji itp.;  dokumentacja zawierająca dane osobowe przechowywana w zamykanych meblach;  dostęp do dokumentów tylko dla osób upoważnionych;  kontrola dostępu do budynku (ochrona, portiernia, system kontroli dostępu itp.);  kontrola dostępu do pomieszczeń (czytnik kart magnetycznych, kod do drzwi itp.);  monitoring wizyjny budynku;  monitoring wizyjny piętra, na którym przechowywane są powierzone dane;  system sygnalizacji włamania i napadu;  system sygnalizacji pożaru; |
| Zabezpieczenia teleinformatyczne | |
|  | Czy każdy użytkownik dostaje imienny identyfikator do systemów informatycznych?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy uprawnienia do przetwarzania danych osobowych są odbierane, gdy kończy się stosunek pracy (lub inna forma współpracy)?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy systemy informatyczne zapewniają wymuszanie na użytkownikach okresowe zmiany haseł oraz zmiany w razie zaistniałej potrzeby?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy wprowadzono ochronę systemów poprzez blokadę komputera, gdy nie jest on używany?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy zapewniono oprogramowanie antywirusowe na stacjach używanych do przetwarzania powierzony danych oraz na urządzeniach mobilnych (np. telefonach)?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy wykorzystywane oprogramowanie posiada licencję i jest na bieżąco aktualizowane?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy stosuje się szyfrowanie urządzeń przenośnych (np. dysków komputerów przenośnych, zewnętrznych pamięci), na których przetwarzane są dane powierzone?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy pracownicy zostali zobowiązani do szyfrowania powierzonych danych osobowych przesyłanych drogą elektroniczną (np. raportowanie)?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy urządzenia mobilne (np. telefony), na których przetwarzane są dane powierzone posiadają skonfigurowaną kontrolę dostępu?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy wykonywane są kopie zapasowe powierzonych danych osobowych zapewniające szybkie przywrócenie dostępu do nich w razie incydentu fizycznego lub technicznego?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy kopie zapasowe są przechowywane w sposób zapewniający bezpieczeństwo powierzonych danych?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
| Analiza ryzyka | |
|  | Czy dokonywana jest okresowa ocena ryzyka dotycząca bezpieczeństwa przetwarzania powierzonych danych osobowych, w szczególności w zakresie zagrożeń:   1. przypadkowego lub niezgodnego z prawem zniszczenia, 2. utraty, modyfikacji, nieuprawnionego ujawnienia, 3. lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.   TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy organizacja wprowadziła, na podstawie oszacowanego ryzyka bezpieczeństwa powierzonych danych, inne środki techniczne i organizacyjne, które nie zostały wymienione powyżej?  *- jeżeli tak, należy wymienić jakie.*  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
| Naruszenia ochrony danych | |
|  | Czy podmiot przetwarzający wdrożył procedury dotyczące zarzadzania incydentami bezpieczeństwa?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy wystąpiły incydenty/naruszenia ochrony danych osobowych przy przetwarzaniu danych powierzonych przez Administratora?  *- jeżeli tak, to w jakim czasie powiadomiono Administratora o naruszeniu?*  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
| Realizacja praw osób fizycznych | |
|  | Czy w ostatnich 24 miesiącach do podmiotu przetwarzającego trafiły jakieś żądania osób fizycznych z art. 12-22 RODO?  *- jeżeli tak, to czy Administrator został o tym poinformowany i w jaki sposób?*  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | W jaki sposób podmiot przetwarzający pomaga Administratorowi wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą w zakresie wykonywania jej praw wynikających z RODO?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy spełniono obowiązek informacyjny z art. 13 lub art. 14 RODO wobec osób, których dane są przetwarzane w związku z powierzeniem danych?  *- jeżeli tak, należy dołączyć wzór stosowanej klauzuli informacyjnej.*  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |

|  |  |
| --- | --- |
| ……………………………………………………………………………..  Data i podpis osoby sporządzającej listę kontrolną | ……………………………………………………………………………..  Data i podpis osoby zatwierdzającej listę kontrolną |