**Załącznik D  
 do Polityki Bezpieczeństwa DO**

**Zakres kontroli (audyt ) ODO**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **L. p.** | **Wymaganie** | **Propozycja pytania audytowego** | **Wskazówka** | **Czy spełniane są wymagania**  **T/N?** |
| 1 | Przetwarzanie danych osobowych jest dopuszczalne wtedy, gdy osoba której dane dotyczą , wyrazi na to zgodę, chyba że przetwarzanie danych jest niezbędne dla ochrony żywotnych interesów osoby której dane dotyczą a uzyskanie jej zgody jest niemożliwe. Dane można przetwarzać do czasu gdy uzyskanie zgody tej osoby będzie możliwe. | Czy osoba której dane dotyczą, wyraziła zgodę na ich przetwarzanie , lub przetwarzanie tych danych jest niezbędne dla ochrony żywotnych interesów tej osoby? | ( UODO art. 23 ust. 1 p1 i ust. 3) Wyjątek stanowi usuwania dotychczasowych |  |
| 2 | Przetwarzanie danych osobowych jest niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. | Czy przetwarzanie danych osobowych jest niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa? | ( UODO art. 23 ust. 1 p2) |  |
| 3 | Przetwarzanie danych osobowych jest konieczne do realizacji umowy , gdy osoba której te dane dotyczą jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą . | Czy są realizowane umowy, z udziałem osoby będącej stroną w umowie lub przetwarzanie danych osobowych jest niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą? | ( UODO art. 23 ust. 1 p3) |  |
| 4 | Przetwarzanie danych osobowych jest niezbędne do wykonywania określonych prawem zadań realizowanych dla dobra publicznego | Czy przetwarzanie danych osobowych jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego? | ( UODO art. 23 ust. 1 p4) |  |
| 5 | Przetwarzanie danych osobowych jest niezbędne dla wypełniania prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie n9ie narusza prawa i wolności osoby n, której dane dotyczą | Czy przetwarzanie danych osobowych jest niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza prawa i wolności osoby, której dane dotyczą ? | (UODO art. 23 ust.1 P5) Zgodnie z UODO art. 23 ust4 za prawnie usprawiedliwiony cel uważa się w szczególności : marketing bezpośredni własnych produktów lub usług administratora danych , dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej. |  |
| 6 | Administrator poinformował osobę o adresie swojej siedziby i pełnej nazwie , a w przypadku gdy administratorem jest osoba fizyczna – o miejscu swego zamieszkania oraz imieniu i nazwisku. | Czy administrator poinformował osobę o adresie swojej siedziby i pełnej nazwie a w , a w przypadku gdy administratorem jest osoba fizyczna- o miejscu swego zamieszkania oraz imieniu i nazwisku? |  |  |
| 7 | Administrator poinformował osobę o celu zbierania danych , a szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych. | Czy administrator poinformował osobę o celu zbierania danych, a szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych? |  |  |
| 8 | Administrator poinformował osobę o prawie dostępu do swoich danych oraz ich poprawiania. | Czy administrator poinformował osobę o prawie dostępu do swoich danych oraz ich poprawiania? |  |  |
| 9 | Administrator poinformował osobę o dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje , o jego prawnej podstawie | Czy administrator poinformował osobę o dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje , o jego podstawie prawnej? |  |  |
| 10 | Administrator poinformował osobę bezpośrednio po utrwaleniu zebranych danych o źródle danych | Czy administrator poinformował osobę o źródle danych ? |  |  |
| 11 | Administrator poinformował osobę bezpośrednio po utrwaleniu zebranych danych o uprawnieniu do wniesienia w określonych ustawowo przypadkach pisemnie umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuacje. | Czy administrator poinformował osobę o uprawnieniu do wniesienia w określonych ustawowo przypadkach pisemnie umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuacje? |  |  |
| 12 | Administrator poinformował osobę bezpośrednio po utrwaleniu zebranych danych o prawie wniesienia sprzeciwu wobec przetwarzania jej danych w określonych ustawowo przypadkach, gdy administrator ma zamiar przetwarzać je w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych | Czy administrator poinformował osobę o prawie wniesienia sprzeciwu wobec przetwarzania jej danych w określonych ustawowo przypadkach, gdy administrator ma zamiar przetwarzać je w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych? |  |  |
| 13 | Administrator zapewnia przetwarzanie danych zgodnie z prawem. | Czy administrator zapewnia przetwarzanie danych zgodnie z prawem? |  |  |
| 14 | Administrator zapewnia , że dane są zbierane dla oznaczonych , zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami. | Czy administrator zapewnia, że dane są zbierane dla oznaczonych , zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami? | Zgodnie z UODO art. 26 ust.2 przetwarzanie danych osobowych w innym celu niż zostały zebrane jest dopuszczalne jeśli nie narusza praw i wolności osoby, której dane dotyczą oraz następuje: w celach badań naukowych, dydaktycznych , historycznych lub statystycznych, z zachowaniem przepisów UODO art. 23 i 25 |  |
| 15 | Administrator zapewnia merytoryczna poprawność danych i adekwatność w stosunku do celów , w jakich są przetwarzane. | Czy administrator zapewnia merytoryczna poprawność danych i adekwatność w stosunku do celów w jakich są przetwarzane? |  |  |
| 16 | Administrator zapewnia, że dane przechowywane są w postaci umożliwiającej identyfikację osób których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania. | Czy administrator zapewnia , ze dane są przechowywane w postaci umożliwiającej identyfikację osób , których dotyczą , nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania ? |  |  |
| 17 | Administrator danych stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną . | Czy administrator danych stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną ? | Zgodnie z UODO art. 39a |  |
| 18 | Administrator danych zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmiana , utratą, uszkodzeniem lub zniszczeniem. | Czy administrator danych zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmiana , utratą, uszkodzeniem lub zniszczeniem |  |  |
| 19 | Administrator danych prowadzi dokumentacje opisującą sposób przetwarzania danych oraz ich środki ochrony. | Czy administrator danych prowadzi dokumentacje opisującą sposób przetwarzania danych oraz ich środki ochrony? |  |  |
| 20 | Dokumentacja zawiera politykę bezpieczeństwa | Czy dokumentacja zawiera politykę bezpieczeństwa? | (Rozp. UODO art. 3 p1) |  |
| 21 | Polityka bezpieczeństwa zawiera w szczególności wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe. | Czy polityka bezpieczeństwa zawiera w szczególności wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe ? |  |  |
| 22 | Polityka bezpieczeństwa zawiera w szczególności wykaz zbiorów danych osobowych wraz z wskazaniem programów zastosowanych do przetwarzania tych danych. | Czy polityka bezpieczeństwa zawiera w szczególności wykaz zbiorów danych osobowych wraz z wskazaniem programów zastosowanych do przetwarzania tych danych ? |  |  |
| 23 | Polityka bezpieczeństwa zawiera w szczególności opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi. | Czy polityka bezpieczeństwa zawiera w szczególności opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi? |  |  |
| 24 | Polityka bezpieczeństwa zawiera w szczególności sposób przepływu danych pomiędzy poszczególnymi systemami. | Czy polityka bezpieczeństwa zawiera w szczególności sposób przepływu danych pomiędzy poszczególnymi systemami ? |  |  |
| 25 | Polityka bezpieczeństwa zawiera w szczególności określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych. | Czy polityka bezpieczeństwa zawiera w szczególności określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych? |  |  |
| 26 | Dokumentacja zawiera instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. | Czy dokumentacja zawiera instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych? | (Rozp. UODO art. 3 p.1 ) |  |
| 27 | Instrukcja zawiera w szczególności procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności | Czy instrukcja zawieraw szczególności procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności ? |  |  |
| 28 | Instrukcja zawiera w szczególności stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem | Czy instrukcja zawiera w szczególności stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem |  |  |
| 29 | Instrukcja zawiera w szczególności procedury rozpoczęcia , zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu. | Czy instrukcja zawiera w szczególności procedury rozpoczęcia , zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu. |  |  |
| 30 | Instrukcja zawiera w szczególności procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania. | Czy instrukcja zawiera w szczególności procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania. |  |  |
| 31 | Instrukcja zawiera w szczególności sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe. | Czy instrukcja zawiera w szczególności sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe. |  |  |
| 32 | Instrukcja zawiera w szczególności sposób, miejsce i okres przechowywania kopii zapasowych | Czy instrukcja zawiera w szczególności sposób, miejsce i okres przechowywania kopii zapasowych |  |  |
| 33 | Instrukcja zawiera w szczególności sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania , którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego. | Czy instrukcja zawiera w szczególności sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania , którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego? | (Rozp. UODO art. 5 p 6 i zał A do Rozp. Pkt III ppkt1) |  |
| 34 | Instrukcja zawiera w szczególności sposób realizacji wymogów dotyczących odnotowania informacji o odbiorcach , którym dane osobowe zostały udostępnione , dacie i zakresie tego udostępnienia. | Czy instrukcja zawiera w szczególności sposób realizacji wymogów dotyczących odnotowania informacji o odbiorcach , którym dane osobowe zostały udostępnione , dacie i zakresie tego udostępnienia? | Wyjątek stanowią systemy Informatyczne używane do przetwarzania danych zawartych w zbiorach jawnych**.** |  |
| 35 | Instrukcja zawiera w szczególności procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych. | Czy instrukcja zawiera w szczególności procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych? |  |  |
| 36 | Dokumentacja jest prowadzona w formie pisemnej | Czy dokumentacja jest prowadzona w formie pisemnej ? | (Rozp. UODO art. 3 p2) |  |
| 37 | Dokumentację wdraża administrator danych. | Czy dokumentację wdraża administrator danych? | ( UODO art. 37) |  |
| 38 | Do przetwarzania danych dopuszczane są wyłącznie osoby posiadające upoważnienie nadane przez administratora danych. | Czy do przetwarzania danych dopuszczane są wyłącznie osoby posiadające upoważnienie nadane przez administratora danych? |  |  |
| 39 | Administrator danych zapewnia kontrolę na tym , jakie dane osobowe, kiedy i przez kogo zostały wprowadzone do zbioru oraz komu są przekazywane. | Czy administrator danych zapewnia kontrolę na tym , jakie dane osobowe, kiedy i przez kogo zostały wprowadzone do zbioru oraz komu są przekazywane? |  |  |
| 40 | Administrator danych prowadzi ewidencje osób upoważnionych do ich przetwarzania. | Czy administrator danych prowadzi ewidencje osób upoważnionych do ich przetwarzania ? | Osoby upoważnione do przetwarzania danych , są Obowiązane do zachowania w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia |  |
| 41 | Ewidencja zawiera imię i nazwisko osoby upoważnionej | Czy ewidencja zawiera imię i nazwisko osoby upoważnionej ? |  |  |
| 42 | Ewidencja zawiera datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych. | Czy ewidencja zawiera datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych ? |  |  |
| 43 | Ewidencja zawiera identyfikator , jeżeli dane są przetwarzane w systemie informatycznym | Czyewidencja zawiera identyfikator , jeżeli dane są przetwarzane w systemie informatycznym |  |  |
| 44 | Obszar ( budynki , pomieszczenia lub części pomieszczeń , tworzących obszar, w którym przetwarzane są dane ) zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. | Obszar ( budynki , pomieszczenia lub części pomieszczeń , tworzących obszar, w którym przetwarzane są dane ) zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych ? | Poziom co najmniej podstawowy stosuje się , gdy :  1)w systemie informatycznym nie są przetwarzane dane , o których mowa w art. 27 ustawy, oraz  2) żadne z urządzeń systemu informatycznego , służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną. |  |
| 45 | Przebywanie osób nieuprawnionych w obszarze ( budynki, pomieszczenia lub części pomieszczeń , tworzących obszar , w którym przetwarzane są dane osobowe) jest dopuszczalne za zgodą administratora danych lub obecności osoby upoważnionej do przetwarzania danych osobowych. | Czy przebywanie osób nieuprawnionych w obszarze ( budynki, pomieszczenia lub części pomieszczeń , tworzących obszar , w którym przetwarzane są dane osobowe) jest dopuszczalne za zgodą administratora danych lub obecności osoby upoważnionej do przetwarzania danych osobowych. | Poziom podstawowy |  |
| 46 | W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych. | Czy w systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych ? | Poziom podstawowy |  |
| 47 | Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają ci najmniej dwie osoby , wówczas zapewnia się , aby w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator. | Czy zapewnia się aby w systemie informatycznym rejestrowany był dla każdego użytkownika odrębny identyfikator? | Poziom podstawowy |  |
| 48 | Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby , wówczas zapewnia się , aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia. | Czy zapewnia się , aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia? |  |  |
| 49 | System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego | Czy system informatyczny służący do przetwarzania danych osobowych zabezpiecza się, przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego ? | Poziom podstawowy |  |
| 50 | System informatyczny służący do przetwarzania danych osobowych zabezpiecza się , przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej. | Czy system informatyczny służący do przetwarzania danych osobowych zabezpiecza się , przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej ? | Poziom podstawowy |  |
| 51 | Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych , nie może być przydzielony innej osobie. | Czy identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych , nie może być przydzielony innej osobie? | Poziom podstawowy |  |
| 52 | W przypadku gdy do uwierzytelnienia użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni | Czy w przypadku gdy do uwierzytelnienia użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni ? | Poziom podstawowy |  |
| 53 | Hasło składa się z co najmniej 6 znaków. | Czyhasło składa się z co najmniej 6 znaków ? | Poziom podstawowy |  |
| 54 | Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. | Czy dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych ? | Poziom podstawowy |  |
| 55 | Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem , modyfikacja , uszkodzeniem lub zniszczeniem. | Czykopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem , modyfikacja , uszkodzeniem lub zniszczeniem? | Poziom podstawowy |  |
| 56 | Kopie zapasowe usuwa się niezwłocznie po ustaniu ich użyteczności. | Czy kopie zapasowe usuwa się niezwłocznie po ustaniu ich użyteczności ? | Poziom podstawowy |  |
| 57 | Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególna ostrożność podczas jego transportu , przechowywania i użytkowania poza obszarem , ( budynki, pomieszczenia lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe) | Czy osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególna ostrożność podczas jego transportu , przechowywania i użytkowania poza obszarem ,w którym przetwarzane są dane osobowe ? | Poziom podstawowy |  |
| 58 | Osoba użytkująca komputer przenośny zawierający dane osobowe , podczas jego transportu stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych. | Czy osoba użytkująca komputer przenośny zawierający dane osobowe , podczas jego transportu stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych? | Poziom podstawowy |  |
| 59 | Urządzenia , dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe , przeznaczone do likwidacji- pozbawia się wcześniej zapisu tych danych , a w przypadku gdy nie jest to możliwe , uszkadza się w sposób uniemożliwiający ich odczytanie. | Czy urządzenia , dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe , przeznaczone do likwidacji- pozbawia się wcześniej zapisu tych danych , a w przypadku gdy nie jest to możliwe , uszkadza się w sposób uniemożliwiający ich odczytanie ? | Poziom podstawowy |  |
| 60 | Urządzenia , dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe , przeznaczone do przekazania podmiotowi nieuprawnionemu do przet3warzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie. | Czy urządzenia , dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe , przeznaczone do przekazania podmiotowi nieuprawnionemu do przet3warzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie? | Poziom podstawowy |  |
| 61 | Urządzenia, dyski lub inne elektroniczne nośniki informacji , zawierające dane osobowe, przeznaczone do naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych. | Czy urządzenia, dyski lub inne elektroniczne nośniki informacji , zawierające dane osobowe, przeznaczone do naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych? | Poziom podstawowy |  |
| 62 | Administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego | Czy administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego ? | Poziom podstawowy |  |
| 63 | W przypadku stosowania haseł do uwierzytelnienia użytkowników , hasła te składają się co najmniej z 8 znaków, zawierają małe i wielkie litery oraz cyfry lub znaki specjalne. | Czyw przypadku stosowania haseł do uwierzytelnienia użytkowników , hasła te składają się co najmniej z 8 znaków, zawierają małe i wielkie litery oraz cyfry lub znaki specjalne? | Poziom ochrony podwyższony.  (Rozp. UODO art. 6 p3) Poziom ten stosuje się gdy : w systemie informatycznym przetwarzane są dane osobowe o których mowa w art. . 27 ustawy, oraz żadne z urządzeń systemu informatycznego , służącego do przetwarzania danych osobowych nie jest podłączone z siecią publiczną |  |
| 64 | Urządzenia i nośniki zawierające dane osobowe przekazywane poza obszar w którym przetwarzane są dane osobowe , zabezpiecza się w sposób zapewniający poufność i integralność tych danych. | Czy urządzenia i nośniki zawierające dane osobowe przekazywane poza obszar w którym przetwarzane są dane osobowe , zabezpiecza się w sposób zapewniający poufność i integralność tych danych ? | Poziom ochrony podwyższony |  |
| 65 | Instrukcję zarządzania systemem informatycznym rozszerza się o sposób stosowania środków bezpieczeństwa dla poziomu podwyższonego. | Czy instrukcję zarządzania systemem informatycznym rozszerza się o sposób stosowania środków bezpieczeństwa dla poziomu podwyższonego ? | Poziom ochrony podwyższony |  |
| 66 | Administrator danych stosuje na poziomie podwyższonym środki bezpieczeństwa, określone dla poziomu podstawowego , o ile zasady określone dla poziomu podwyższonego nie stanowią inaczej. | Czy administrator danych stosuje na poziomie podwyższonym środki bezpieczeństwa, określone dla poziomu podstawowego , o ile zasady określone dla poziomu podwyższonego nie stanowią inaczej ? | Poziom ochrony podwyższony |  |
| 67 | Wdrożono fizyczne lub logiczne zabezpieczenia chroniące, przed nieuprawnionym dostępem z sieci publicznej , system informatyczny służący do przetwarzania danych osobowych. | Czy wdrożono fizyczne lub logiczne zabezpieczenia chroniące, przed nieuprawnionym dostępem z sieci publicznej , system informatyczny służący do przetwarzania danych osobowych? | Poziom wysoki stosuje się , gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną. |  |
| 68 | W przypadku zastosowania logicznych zabezpieczeń obejmują one kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną. | Czy w przypadku zastosowania logicznych zabezpieczeń obejmują one kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną? | Poziom wysoki |  |
| 69 | W przypadku zastosowania logicznych zabezpieczeń obejmują one kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych. | Czyw przypadku zastosowania logicznych zabezpieczeń obejmują one kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych ? | Poziom wysoki |  |
| 70 | Administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej. | Czy administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej ? | Poziom wysoki |  |
| 71 | Administrator danych stosuje środki bezpieczeństwa określone dla poziomu podstawowego i podwyższonego , o ile zasady określone dla poziomu wysokiego nie stanowią inaczej. | Czy administrator danych stosuje środki bezpieczeństwa określone dla poziomu podstawowego i podwyższonego , o ile zasady określone dla poziomu wysokiego nie stanowią inaczej ? | Poziom wysoki |  |
| 72 | System informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie daty pierwszego wprowadzenia danych do systemu. | Czy system informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie daty pierwszego wprowadzenia danych do systemu ? |  |  |
| 73 | System informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie identyfikatora użytkownika wprowadzającego dane osobowe do systemu. | Czy system informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie identyfikatora użytkownika wprowadzającego dane osobowe do systemu ? | Chyba , że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłączenie jedna osoba**.** |  |
| 74 | System informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie źródła danych, w przypadku zbierania danych , nie od osoby , której one dotyczą . | Czy system informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie źródła danych, w przypadku zbierania danych , nie od osoby , której one dotyczą ? |  |  |
| 75 | System informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie informacji o odbiorcach, którym dane osobowe zostały udostępnione , dacie i zakresie tego udostępnienia , chyba , że system informatyczny używany jest do przetwarzania danych, zawartych w zbiorach jawnych. | Czy system informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie informacji o odbiorcach, którym dane osobowe zostały udostępnione , dacie i zakresie tego udostępnienia , chyba , że system informatyczny używany jest do przetwarzania danych, zawartych w zbiorach jawnych ? | Zgodnie z UODO art. 7 p6 za odbiorcę uważa się każdego , komu udostępnia się dane osobowe , z wyłączeniem : osoby , której dane dotyczą : osoby upoważnionej do przetwarzania danych, przedstawiciela (UODO art. 31a) , podmiotu ( UODO art. 31) , organów państwowych lub organów samorządu terytorialnego , którym dane są udostępniane w związku z prowadzonym postępowaniem |  |
| 76 | System informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie sprzeciwu wobec przetwarzania danych przez osobę której te dane dotyczą . | Czysystem informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie sprzeciwu wobec przetwarzania danych przez osobę której te dane dotyczą ? |  |  |
| 77 | Odnotowanie informacji dotyczących daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika wprowadzającego te dane następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych. | Czy odnotowanie informacji dotyczących daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika wprowadzającego te dane następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych ? |  |  |
| 78 | System umożliwia tworzenie i drukowanie raportów zawierających odnotowane informacje w przystępnej formie dla każdej osoby , której dane są przetwarzane**.** | Czy system umożliwia tworzenie i drukowanie raportów zawierających odnotowane informacje w przystępnej formie dla każdej osoby , której dane są przetwarzane**?** |  |  |
| **CZĘŚĆ PRAKTYCZNA PYTAŃ KONTROLNYCH** | | | | |
| 1 | Wyznaczona przez administratora danych osoba , nadzorująca przestrzeganie zasad ochrony danych osobowych | Czy powołano Administratora Bezpieczeństwa Informacji? | Możliwe zabezpieczenia organizacyjne |  |
| 2 |  | Czy określono zakres obowiązków Administratora Bezpieczeństwa Informacji? | Możliwe zabezpieczenia organizacyjne |  |
| 3 |  | Czy określono Instrukcję postępowania w przypadku naruszenia ochrony danych osobowych? | Możliwe zabezpieczenia organizacyjne |  |
| 4 |  | Czy korespondencja w zakresie procedur kadrowo- płacowych prowadzona jest za pomocą listów poleconych ? | Możliwe zabezpieczenia organizacyjne |  |
| 5 |  | Czy pracownicy ( użytkownicy) dopuszczeni do przetwarzania danych osobowych zapoznali się z polityką bezpieczeństwa? | Możliwe zabezpieczenia osobowe |  |
| 6 |  | Czy pracownicy (użytkownicy) dopuszczeni do przetwarzania danych osobowych zapoznali się z instrukcją zarządzania? | Możliwe zabezpieczenia osobowe |  |
| 7 |  | Czy pracownicy zachowują ostrożność udzielając informacji dot. danych osobowych przez telefon i poza organizacją? | Możliwe zabezpieczenia osobowe |  |
| 8 |  | Czy pracownicy zachowują ostrożność udzielając informacji osobom nieuprawnionym? | Możliwe zabezpieczenia osobowe |  |
| 9 |  | Czy pracownicy reagują na obecność nieznanych osób przebywających w pobliżu miejsca przetwarzania danych i zachowujące się podejrzanie? | Możliwe zabezpieczenia osobowe |  |
| 10 |  | Czy pracownicy są świadomi zgłaszania incydentów bezpieczeństwa Administratorowi bezpieczeństwa informacji? | Możliwe zabezpieczenia osobowe |  |
| 11 |  | Czy pracownicy podpisali oświadczenia? | Możliwe zabezpieczenia osobowe |  |
| 12 |  | Czy zakres udostępnionych danych osobowych osobie upoważnionej do przetwarzania danych osobowych jest pisemnie potwierdzony przez Administratora Danych Osobowych? | Możliwe zabezpieczenia osobowe |  |
| 13 |  | Czy przestrzegany jest zakaz niepodawania swojego hasła , pod rygorem naruszenia zasad bezpieczeństwa informacji? | Możliwe zabezpieczenia osobowe |  |
| 14 |  | Czy hasło posiada ilość znaków, zgodnie z poziomem bezpieczeństwa? |  |  |
| 15 |  | Czy hasła nie są zapisywane na kartkach, w pobliżu komputera , w innych widocznych miejscach? | Możliwe zabezpieczenia osobowe |  |
| 16 |  | Czy użytkownik jest świadom zakazu udostępniania swojego hasła innym użytkownikom? | Możliwe zabezpieczenia osobowe |  |
| 17 |  | Czy sprawdzane jest podczas logowania się , czy ktoś się nie próbował włamać do systemu? | Możliwe zabezpieczenia osobowe |  |
| 18 |  | Czy użytkownik loguje się zawsze na swój login i hasło? | Możliwe zabezpieczenia osobowe |  |
| 19 |  | Czy użytkownik blokuje dostęp do swojego komputera po odejściu od stanowiska pracy za pomocą wygaszacza z hasłem | Możliwe zabezpieczenia osobowe |  |
| 20 |  | Czy po zakończeniu pracy użytkownik wylosowuje się a następnie zamyka komputer? | Możliwe zabezpieczenia osobowe |  |
| 21 |  | Czy w razie awarii lub sprzętu przetwarzającego dane osobowe, użytkownik powiadamia informatyka , do którego kontakt jest znany? | Możliwe zabezpieczenia osobowe |  |
| 22 |  | Czy laptop pozostawiony jest bez opieki w pomieszczeniu , jeśli pomieszczenie nie jest zamknięte na klucz? | Możliwe zabezpieczenia osobowe |  |
| 23 |  | Czy ekrany monitorów ustawiono w taki sposób , żeby uniemożliwić odczyt wyświetlanych danych osobowych osobom nieupoważnionym? | Możliwe zabezpieczenia osobowe |  |
| 24 |  | Czy określono politykę korzystania z Internetu? | Możliwe zabezpieczenia osobowe |  |
| 25 |  | Czy określono politykę korzystania z poczty firmowej? | Możliwe zabezpieczenia osobowe |  |
| 26 |  | Czy zarząd / kierownictwo najwyższego szczebla jest świadome odpowiedzialności karnej za naruszenie Ochrony Danych Osobowych ? | Możliwe zabezpieczenia osobowe |  |
| 27 |  | Czy dokumenty w postaci papierowej lub elektronicznej zawierające dane osobowe po zakończeniu pracy są zamknięte? | Możliwe zabezpieczenia fizyczne |  |
| 28 |  | Czy dokumenty papierowe i CD zawierające dane osobowe niszczone są w niszczarkach? | Możliwe zabezpieczenia fizyczne |  |
| 29 |  | Czy stosuje się system kontroli dostępu? | Możliwe zabezpieczenia fizyczne |  |
| 30 |  | Czy konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych jedynie za pośrednictwem aplikacji ? | Możliwe zabezpieczenia techniczne |  |
| 31 |  | Czy określono zasady działania programów antywirusowych wraz z odpowiedziami użytkowników? | Możliwe zabezpieczenia techniczne |  |
| 32 |  | Czy używane jest tylko licencjonowane oprogramowanie do przetwarzania danych osobowych? | Możliwe zabezpieczenia techniczne |  |
| 33 |  | Czy urządzenia wchodzące w skład systemu informatycznego podłączone są do odrębnego obwodu elektrycznego, zabezpieczonego na wypadek zaniku napięcia albo awarii w sieci zasilającej? | Możliwe zabezpieczenia techniczne |  |
| 34 |  | Czy sieć lokalna podłączona jest do Internetu za pomocą odrębnego komputera? | Możliwe zabezpieczenia techniczne |  |