AUDYT OCHRONY DANYCH OSOBOWYCH (RODO) – LISTA KONTROLNA

Zawartość

Proszę o zaznaczenie X w miejscu właściwej odpowiedzi. Czasami można też podkreślić lub zakreślić właściwą informację, jeśli podane są przykłady. W razie potrzeby lub w razie wskazania, można umieścić komentarz.

ZAGADNIENIA OGÓLNE

1. Ile osób jest zatrudnionych w firmie?

……. *[Liczba]* ☐ PRACOWNIKÓW ☐ WŁAŚCICIEL (JDG) ☐ NIE WIEM

2. Czy firma przetwarza dane osobowe inne niż swoich pracowników, np. współpracowników, osób zatrudnionych na podstawie umowy o dzieło ? *[podkreśl właściwe lub dopisz]*

☐ TAK ☐ NIE ☐ NIE WIEM

……..

3. Jaki rodzaj Klientów posiada firma? *[dopisz lub zakreśl właściwe]*

Osoby fizyczne/ konsumenci/ przedsiębiorcy/ klienci online

……

……

4. Jaka jest szacunkowa ilość danych osobowych przetwarzanych przez firmę? Jakie dane osobowe posiada Firma? *[dopisz lub zakreśl właściwe]*

……

……

Klienci/ kontrahenci/ dane osób zapisanych na newsletter/ formularz kontaktowy na stronie/ dane w „chmurze" np. Dropbox/ korespondencja mailowa/ skrzynka mailowa na własnym serwerze/ skrzynka mailowa na cudzym serwerze np. gmail/ reklamacje/ wysyłanie potwierdzeń spotkań sms-em lub e-mailem – baza kontaktów/ rejestr klientów np. w Excelu/ ZUS/ US/ rejestr pracowników/ rekrutacja pracowników/ osoby z fanpage/ osoby z grupy na Facebooku/ klienci ze sklepu online/ osoby z dodatkowej platformy/ Inne (jakie?)

……

……

……

5. Jaką dokumentację posiada Firma związaną z ochroną danych osobowych? Czy Firma podjęła jakiekolwiek kroki związane z ochroną danych osobowych? Jakie?

……

……

……

……

6. Jakie kategorie danych osobowych są przetwarzane przez Firmę? *[zakreśl właściwe] Np. Imię/ nazwisko/ adres/ e-mail/ numer telefonu/ PESEL/ NIP/ numer dowodu osobistego lub innego dokumentu (jakiego?) ……../preferencje (jakie?) ..…….. wykształcenie/ wiek/ data urodzenia/ pochodzenie/ stan cywilny/ rasa/ Nick z fanpage na Facebooku lub z innych mediów społecznościowych (jakich?)……*

..……..……..,

dane na fakturach podane przez klientów w systemie do fakturowania (jakim?) ……..

……..……..

Inne (jakie?) ……..

7. Czy Firma posiada jakiekolwiek firmy zależne? *[zakreśl właściwe]*

☐ TAK *Spółki córki/ spółki matki/ spółki cywilne/ inne……..……..*

☐ NIE

8. Jaka jest wewnętrzna struktura Firmy? *[zakreśl właściwe]*

Właściciel/ pracownicy/ prezes zarządu/ rada nadzorcza/ komisja rewizyjna/ współpracownicy/ osoby pracujące na zlecenie – freelancerzy/ inne……..

9. W ilu lokalizacjach Firma prowadzi działalność związaną z przetwarzaniem danych osobowych? Jaki jest to rodzaj działalności? …….

.....

10. Czy Firma zleca jakieś czynności na zasadach outsourcingu? Czy wiąże się z tym przekazywanie danych osobowych? *[zakreśl właściwe]*

☐ TAK : *Księgowa/ informatyk/ kurierzy/ poczta polska/ Inne ……*

☐ NIE

11. Z jakich aplikacji lub zewnętrznych platform korzysta firma?

Facebook/ fanpage na Facebooku/ Instagram/ LinkedIn/ Dropbox/ OneDrive/ Poczta gmail biznesowa lub osobista (jaka?)/ SignRequest / Fakturownia/ Hosting zewnętrzny (gdzie?) ……/ domena (gdzie?) ……..……/ Dostawca newslettera (jaki?)……/ Wirtualna asystentka/ Firma rekrutująca pracowników/ Specjalista BHP/ Ubezpieczyciel lub agent ubezpieczeniowy/ Sklep online: Przelewy24/ TPay/ Platforma sklepu online zarządzana przez zewnętrznego dostawcę/ Inne ……....

……

12. Czy firma korzysta ze służb ochrony oraz personelu sprzątającego – „własnego" czy „zewnętrznego"?

☐ WŁASNY ☐ ZEWNĘTRZNY ☐ NIE KORZYSTA

13. Czy firma posiada własną infrastrukturę IT, w tym serwery?

☐ TAK ☐ NIE ☐ NIE WIEM ☐ SERWER JEST ZEWNĘTRZNY

Jaka jest ilość serwerowni?

……

Jakie usługi działają na serwerach?

……

Jakie usługi działają na ewentualnym hostingu?

……

14. Czy przedstawiciele podmiotów zewnętrznych mają wstęp do pomieszczeń firmy?

☐ TAK ☐ NIE ☐ NIE WIEM

Kto? W jakim celu? ……

15. Ile systemów informatycznych służy do przetwarzania informacji?

……

16. Czy firma przechodziła kiedykolwiek audyt bezpieczeństwa informacji?

☐ TAK ☐ NIE ☐ NIE WIEM

17. Czy firma posiada wdrożone normy ISO np. 9001, 27001?

☐ TAK ☐ NIE ☐ NIE WIEM

POZIOM ZABEZPIECZEŃ ORGANIZACYJNYCH

1. Czy zostały opracowane polityka bezpieczeństwa oraz instrukcja zarządzania systemami informatycznymi?

☐ TAK ☐ NIE ☐ NIE WIEM

2. Czy oba dokumenty są zgodne z obowiązującymi przepisami?

☐ TAK ☐ NIE ☐ NIE WIEM

3. Czy osoby dopuszczone do przetwarzania danych osobowych otrzymały pisemne upoważnienia (na tym etapie sprawdza się tylko, czy administrator danych osobowych wystawia takie upoważnienia i czy ich wzór jest zgodny z przyjętym i obowiązującym w Firmie)?

☐ TAK ☐ NIE ☐ NIE WIEM

4. Czy wszystkie osoby, które mają dostęp do danych osobowych zostały zapoznane z przepisami oraz wewnętrznymi dokumentami z zakresu ochrony danych osobowych (Klient powinien mieć ich oświadczenia w tym zakresie)?

☐ TAK ☐ NIE ☐ NIE WIEM

5. Czy prowadzona jest ewidencja upoważnień do przetwarzania danych osobowych?

☐ TAK ☐ NIE ☐ NIE WIEM

6. Czy ewidencja jest zgodna z posiadanymi upoważnieniami – czy jest aktualizowana?

☐ TAK ☐ NIE ☐ NIE WIEM

7. Czy osoby mające dostęp do danych zostały przeszkolone w zakresie zabezpieczeń systemu informatycznego?

☐ TAK ☐ NIE ☐ NIE WIEM

8. Czy osoby zatrudnione/pracujące przy przetwarzaniu danych zostały zobowiązane do zachowania danych w tajemnicy?

☐ TAK ☐ NIE ☐ NIE WIEM

7. Czy Administrator stosuje politykę tzw. czystego biurka?

☐ TAK ☐ NIE ☐ NIE WIEM

9. Czy kopie zapasowe danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe są na bieżąco przetwarzane?

☐ TAK ☐ NIE ☐ NIE WIEM ☐ SĄ W CHMURZE

POZIOM ZABEZPIECZEŃ TECHNICZNYCH - SPRAWDZENIE BEZPIECZEŃSTWA TELEINFORMATYCZNEGO.

1. Czy w Firmie funkcjonują zasady nadawania/zmieniania/odbierania uprawnień do systemów informatycznych?

☐ TAK ☐ NIE ☐ NIE WIEM

2. Czy obowiązują i są przestrzegane zasady rozpoczęcia i zakończenia pracy w systemie / przy komputerze?

☐ TAK ☐ NIE ☐ NIE WIEM

3. Czy pracownicy blokują system, podczas opuszczenia stanowiska pracy w trakcie dnia pracy?

☐ TAK ☐ NIE ☐ NIE WIEM

4. Czy komputery mają ustawione przechodzenie w stan uśpienia/ wylogowują się i po jakim czasie?

☐ TAK ☐ NIE ☐ NIE WIEM

Czas: ……..

5. Czy osoby dopuszczone do pracy w systemie mają nadane odpowiednie upoważnienia na piśmie?

☐ TAK ☐ NIE ☐ NIE WIEM

6. Czy stosuje się identyfikatory i hasła dla użytkowników zgodnie z wymogami formalnymi określonymi w Polityce Ochrony Danych Osobowych/ Polityce Bezpieczeństwa?

☐ TAK ☐ NIE ☐ NIE WIEM

7. Czy systemy informatyczne służące do przetwarzania danych osobowych zapewniają odpowiedni poziom ochrony przed osobami trzecimi? Jakie są w tym zakresie stosowane zabezpieczenia?

☐ TAK ☐ NIE ☐ NIE WIEM

(trudne hasła, zmieniane regularnie co ……... dni/ procedury odbioru haseł i upoważnień/ inne……..….)

8. Czy sam sprzęt komputerowy jest odpowiednio zabezpieczony systemowo i fizycznie (np. przed wyniesieniem)?

☐ TAK ☐ NIE ☐ NIE WIEM

Jak? ……....

9. Czy tworzone są kopie zapasowe i czy umożliwiają odzyskanie danych? Jak często?

☐ TAK ☐ NIE ☐ NIE WIEM

……...

10. Czy systemy służące do przetwarzania danych osobowych odnotowują wszelkie czynności wykonywane na danych osobowych przez użytkowników?

☐ TAK ☐ NIE ☐ NIE WIEM

Jak? ……....

11. Czy pracownicy niszczą dane wygenerowane z systemów, gdy są już niepotrzebne?

☐ TAK ☐ NIE ☐ NIE WIEM ☐ NIE DOTYCZY

Jak? ……

12. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone za pomocą niszczarek dokumentów.

☐ TAK ☐ NIE ☐ NIE WIEM

Jak?……

13. Praca na danych odbywa się :

Wyłącznie za pomocą komputera/ również w formie papierowej/ Inne ……..

14. Czy Firma korzysta z Internetu, przetwarzając dane osobowe?

☐ TAK ☐ NIE ☐ NIE WIEM

15. Jak Firma chroni połączenie internetowe?

Środki kryptograficznej ochrony danych/ Firewall/ macierz dyskowa/ system IDS/IPS do ochrony dostępu do sieci komputerowej/ procedura oddzwonienia (callback)/ proces uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła/ hasło BIOS/ mechanizm wymuszający okresową zmianę haseł/ system operacyjny pozwalający na określenie odpowiednich praw dostępu do zasobów informatycznych dla poszczególnych użytkowników systemu informatycznego/ system rejestracji dostępu do zbioru danych osobowych/ oprogramowanie zabezpieczające przed nieuprawnionym dostępem do systemu informatycznego/ oprogramowanie umożliwiające wykonanie kopii zapasowych zbiorów danych osobowych/ środki umożliwiające określenie praw dostępu do zbioru danych osobowych/ Dostęp do zbioru danych osobowych zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła/ Zastosowano kryptograficzne środki ochrony danych osobowych np. certyfikat ssl/ Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych/ Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe/ Zastosowano mechanizm blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

POZIOM ZABEZPIECZEŃ NA STRONIE WWW

1. Czy strona posiada informację o cookies (ciasteczkach)?

☐ TAK ☐ NIE ☐ NIE WIEM

2. Czy strona posiada politykę cookies?

☐ TAK ☐ NIE ☐ NIE WIEM

3. Czy strona posiada politykę prywatności?

☐ TAK ☐ NIE ☐ NIE WIEM

4. Czy informacja o polityce prywatności odsyła do linku (interaktywny link, hiperłącze)?

☐ TAK ☐ NIE ☐ NIE WIEM

5. Czy zbierane są zapisy na newsletter?

☐ TAK ☐ NIE ☐ NIE WIEM

6. Czy masz ustawioną podwójną weryfikację nowego subskrybenta, tzw. double opt-in?

☐ TAK ☐ NIE ☐ NIE WIEM

7. Jakie dane zbierane są przy zapisie na newsletter? *[zakreśl właściwe]*

Imię/ nazwisko / e-mail/ data urodzenia/ Inne (jakie?) ……

……..…….....

8. Czy przy zapisie na newsletter istnieje opcja zaznaczenia checkboxów? Jeśli tak to jakich?

☐ TAK ☐ NIE ☐ NIE WIEM

……

……

9. Czy checkboxy są zaznaczone z góry?

☐ TAK ☐ NIE ☐ NIE WIEM

10. Czy checkboxy są zrozumiałe?

☐ TAK ☐ NIE ☐ NIE WIEM

11. Czy istnieją strony lądowania? Jeśli tak to jakie (proszę podać ich adres/ link oraz informację czy są aktywne)

☐ TAK ☐ NIE ☐ NIE WIEM ☐ WSZYSTKIE AKTYWNE

……

……

12. Czy na stronie jest umieszczona klauzula informacyjna RODO?

☐ TAK ☐ NIE ☐ NIE WIEM

W jakim miejscu?

……

13. Czy wysłałeś do bazy swoich kontaktów treść klauzuli informacyjnej? Kiedy?

☐ TAK ☐ NIE ☐ NIE WIEM

……

14. Czy chcesz wysyłać do swoich klientów sms-y oraz e-maile marketingowe/ handlowe?

☐ TAK ☐ NIE ☐ NIE WIEM ☐ E-MAIL ☐ SMS

15. Czy zbierasz na to dodatkowe zgody?

☐ TAK ☐ NIE ☐ NIE WIEM

16. Czy link dezaktywacyjny w newsletterze (do wypisania się z newslettera) jest aktywny/ działa?

☐ TAK ☐ NIE ☐ NIE WIEM

17. Czy posiadasz na stronie formularz kontaktowy?

☐ TAK ☐ NIE ☐ NIE WIEM

POZIOM ZABEZPIECZEŃ FIZYCZNYCH

1. Gdzie przechowywane są dane? *[opisz i zakreśl właściwe]*

Pokój wydzielony/ biuro zamykane na klucz/ pokój współdzielony z innymi osobami/ zamykana na klucz szafa/ monitoring/ system kontroli/ drzwi antywłamaniowe/ dom zabezpieczony alarmem/ Inne ……..

2. Gdzie przechowywane są kopie zapasowe? *[zakreśl właściwe]*

Sejf/ zamykana szafa metalowa/ niemetalowa/ kasa pancerna

3. Jak pomieszczenie biurowe chronione jest przed pożarem? *[zakreśl właściwe]*

Gaśnica/ system antypożarowy/ Inne……....

Nota prawna