ŚRODKI BEZPIECZEŃSTWA INFORMACJI

Dane Podmiotu Przetwarzającego:

Nazwa	Medicover Sp. z o. o.
Adres	Al. Jerozolimskie 96, 00-807 Warszawa
NIP	525-15-77-627

Lp.	Treść pytania	Odpowiedź:
1.	Czy podmiot przetwarzający dane osobowe („PPDO") przetwarza dane o stanie zdrowia lub inne kategorie danych zaliczanych do danych sensytywnych?	Tak
2.	Czy PPDO wyznaczył Inspektora Ochrony Danych?	Tak
3.	Czy PPDO wprowadził środki techniczne i organizacyjne, które będą spełniały wymogi RODO oraz innych aktów regulujących legalne przetwarzanie danych osobowych oraz będą chroniły prawa osób, których dane dotyczą?	Tak
4.	Czy PPDO korzysta z dalszych procesorów w procesie przetwarzania danych osobowych na zlecenie administratora danych osobowych?	Tak
4a.	Jeżeli PPDO korzysta z dalszych procesorów, to czy ma z nimi podpisane umowy powierzenia przetwarzania danych zapewniające te same obowiązki ochrony danych jak w umowie pomiędzy PPDO a Administratorem Danych?	Tak
4b.	Czy dalsi procesorzy stosują środki techniczne i organizacyjne spełniające wymogi RODO?	Tak
4c.	Jeżeli PPDO korzysta z dalszych procesorów to czy są oni zlokalizowani w ramach EOG?	Tak
	Kwestie proceduralne	
1.	Czy PPDO prowadzi rejestr czynności dla powierzonych operacji przetwarzania danych osobowych?	Tak
2.	Czy PPDO przeprowadził ocenę skutków dla ochrony danych?	Tak
3.	Czy PPDO wdrożył procedury dotyczące zarzadzania incydentami bezpieczeństwa?	Tak
4.	Czy PPDO przewidział środki pomagające administratorowi danych osobowych wywiązać się z jego obowiązków określonych w rozdziale III RODO oraz w art. 32-36 RODO.	Tak
	Kwestie bezpieczeństwa	
1.	Czy PPDO przechodzi regularne audyty z zakresu bezpieczeństwa danych?	Tak
2.	Czy PPDO zapewnia, że osoby upoważnione do przetwarzania danych są zobowiązane do zachowania tajemnicy?	Tak

Tabela nr.1 Stosowane środki techniczne i organizacyjne

Środki techniczne i organizacyjne
Proszę wskazać stosowane środki techniczne i organizacyjne służące do uwierzytelniania i autoryzacji użytkowników oraz transmisji danych w systemach IT służących do przetwarzania danych osobowych.
Odpowiedź: Każdy użytkownik posiada indywidualny login oraz hasło do logowania do systemów. Transmisja danych zabezpieczona jest protokołem SSH. Zdalny dostęp do systemów zabezpieczony jest dodatkowo drugim środkiem uwierzytelniającym w postaci generowanego tokenu.
Proszę opisać proces stałego monitorowania, gromadzenia i zarządzania incydentami bezpieczeństwa w systemach przetwarzających dane Osobowe.

Odpowiedź: Każdy pracownik, współpracownik Medicover sp. Z o.o. , który jest uczestnikiem bądź świadkiem naruszenia zasad bezpieczeństwa informacji lub podejrzewa taką sytuację jest zobowiązany do niezwłocznego zgłoszenia zaistniałej sytuacji do Inspektora Ochrony danych. Pracownik/współpracownik zgłasza naruszenie bezpieczeństwa informacji bezpośrednio do IOD lub przy wsparciu przełożonego. Naruszenie można zgłosić na adres mailowy IOD, poprzez formularz online znajdujący się na stronie intranet, drogą telefoniczną lub osobiście do IOD. IOD ewidencjonuje wszystkie otrzymane zgłoszenia w rejestrze naruszeń bezpieczeństwa informacji. Rejestr naruszeń bezpieczeństwa informacji prowadzony jest w formie elektronicznej.
Proszę opisać, metody i środki techniczne i organizacyjne stosowane do realizacji procesów backupowych.
Odpowiedź: Kopie zapasowe wykonywane są dla systemów informatycznych używanych w Medicover, które zawierają dane lub ich utworzenie od nowa przekracza oczekiwany czas odtworzenia RTO. Kopie zapasowe regularnie poddawane są sprawdzeniu możliwości odtworzenia. Testowanie odtwarzania podlega rejestracji. Kopie zapasowe wykonywane są na dedykowane urządzania backupowe zlokalizowane w dwóch centrach danych. Urządzenia synchronizują się między sobą w sposób asynchroniczny bazując na zmienionych blokach danych.
Proszę opisać i wskazać metody, w jaki sposób prowadzony jest nadzór w sytuacji dostępu do systemów przetwarzających Dane Osobowe przez stronę trzecią, podwykonawcę.
Odpowiedź: Osoba odpowiedzialna za kontakt ze strony Medicover występuje do Działu ds. Bezpieczeństwa Informacji z wnioskiem o przydzielenie zewnętrznemu kontrahentowi uprawnień, które umożliwiają realizację kontraktu zgodnie z zakresem w umowie. Zakres uprawnień niezbędnych do realizacji kontraktu wskazuje kontrahent a zatwierdza Administrator IT. Dział bezpieczeństwa Informacji po zatwierdzeniu wnioskowanych uprawnień zleca ich przydzielenie odpowiednim zespołom, które są odpowiedzialne za poszczególne obszary. Każdy pracownik kontrahenta mający dostęp do zasobów Medicover musi posiadać swój unikalny login w celu uzyskania dostępu do zasobów Medicover. Każdy kontrahent uzyskujący dostęp do zasobów Medicover jest zobowiązany do zachowania poufności. Zdalny dostęp dla kontrahentów realizowany jest za pośrednictwem VPN po uprzednim połączeniu ze stacją monitorującą, która zapisuje całą sesję użytkownika.
Proszę określić miejsca przetwarzania i lokowania danych osobowych w systemach IT.
Odpowiedź: Infrastruktura Własna, Data Center mieszące się w Warszawie, ATM również w Warszawie.
Czy kiedykolwiek, podlegaliście Państwo audytom bezpieczeństwa IT wykonywanym przez zewnętrzne podmioty?
Odpowiedź: TAK, regularnie. Dla istniejących aplikacji zewnętrznych raz do roku, dla nowych aplikacji przed wdrożeniem.
Czy posiadacie Państwo wdrożoną i stosowaną procedurę trwałego niszczenia nośników danych zawierających dane osobowe?
Odpowiedź: Tak, jest Procedura zarządzania cyklem życia aktywów IT.
Proszę o opisanie mechanizmu zarządzania rolami i profilami uprawnień użytkowników w systemach przetwarzających dane osobowe.
Odpowiedź: Dział bezpieczeństwa informacji odpowiada za okresową weryfikacją aktywnych dostępów w systemach informatycznych Medicover. Weryfikacja aktywnych dostępów w systemach odbywa się we współpracy z Administratorami Biznesowymi poszczególnych systemów. W przypadku gdy na liście znajdują się osoby niepracujące Dział Bezpieczeństwa Informacji zgłasza do Administratora danego systemu wniosek o dezaktywację kont użytkowników i aktualizację listy pracowników. Dodatkowo, dla wszystkich stanowisk opracowane zostały profile stanowiskowe, które definiują niezbędny zakres uprawnień na danym stanowisku pracy. Ewentualne modyfikacje w uprawnieniach odbywają się tylko za zgodą przełożonego, Administratora Biznesowego, oraz po podaniu uzasadnienia.
Czy system zapewnia możliwość pseudonimizacji i szyfrowania danych?
Odpowiedź: TAK

SŁOWNIK:

1) **Administrator Danych** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych zgodnie z art. 4 ust. 7 RODO;
2) **Arkusz Weryfikacyjny** – Arkusz przekazywany Przetwarzającemu do wypełnienia w związku ze świadczeniem usług na rzecz Administratora Danych;
3) **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na jeden lub kilka specyficznych czynników ją określających;
4) **Inspektor Ochrony Danych, IOD** – osoba wyznaczona przez Administratora Danych zgodnie z art. 37 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 (ogólne rozporządzenie o ochronie danych osobowych), odpowiedzialna za zapewnienie przestrzegania przepisów o ochronie danych osobowych w spółce Administratora Danych;
5) **Przetwarzanie danych osobowych** – oznacza jakiekolwiek operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
6) **Podmiot przetwarzający, Przetwarzający** – Medicover Sp. z o.o. z siedzibą w Warszawie (kod pocztowy: 00-807) przy Al. Jerozolimskie 96, zarejestrowana w Sądzie Rejonowym dla m.st. Warszawy, XII Wydział Krajowego Rejestru Sądowego. KRS: 0000021314 NIP: 525-15-77-627 Kapitał zakładowy: 36 000 000, 00 złotych.;
7) **RODO** – 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 (ogólne rozporządzenie o ochronie danych osobowych);
8) **Umowa powierzenia przetwarzania** – podstawa prawna powierzenia przetwarzania danych osobowych na zlecenie Administratora Danych, zawarta zgodnie z wymaganiami wskazanymi w art. 28 RODO.