

Administrator: MESKO S.A.

ul. Legionów 122, 26-111 Skarżysko-Kamienna

Lista kontrolna dla podmiotu przetwarzającego zgodnie z art. 28 RODO

Dane podmiotu przetwarzającego

Nazwa:

Adres:

Data wypełnienia dokumentu:

Podmiot przetwarzający jest zobligowany do wdrożenia i stosowania mechanizmów pozwalających wykazać zgodność z RODO. Poniższa lista kontrolna umożliwi weryfikację wybranych obszarów oraz wdrożonych zasad przetwarzania danych w kontekście zgodności z RODO.

Uprzejmie prosimy o udzielenie wyczerpujących odpowiedzi na pytania w poniższej tabeli oraz dołączenie załączników, jeżeli jest to konieczne.

Lp.	Pytanie	Odpowiedź
1.	Działania organizacyjne	
a.	Czy wyznaczono Inspektora Ochrony Danych (IOD) lub osobę odpowiedzialną za obszar ochrony danych? Jeżeli IOD nie został wyznaczony, czy dokonano analizy pod kątem obowiązku wyznaczenia IOD i czy analiza ta została udokumentowana? <i>Podaj kontakt do IOD, a w razie niewyznaczenia IOD wskaż uzasadnienie jego niewyznaczenia.</i>	
b.	Czy pracownicy, którzy będą przetwarzać powierzone dane, mają wydane upoważnienia do przetwarzania danych osobowych?	
c.	Czy osoby upoważnione do przetwarzania danych zobowiązały się do zachowania tajemnicy informacji dotyczących przetwarzanych danych oraz tajemnicy informacji o ich zabezpieczeniu?	
d.	Czy przeprowadzane są dla pracowników i innych osób przetwarzających dane osobowe szkolenia zwiększające świadomość z zakresu ochrony danych osobowych? <i>Podaj zasady i podaj datę ostatniego szkolenia.</i>	
e.	Czy wdrożono zasady realizacji praw podmiotów danych (do informacji o przetwarzaniu, dostępu do danych oraz ich kopii, do sprostowania lub uzupełnienia danych, do usunięcia danych, do ograniczenia przetwarzania, do przenoszenia danych, do sprzeciwu, do niepodlegania wyłącznie zautomatyzowanym decyzjom ostatecznym)? <i>Opisz proces realizacji prawa.</i>	

- f. Czy wdrożono politykę ochrony danych i zasady zarządzania systemami informatycznymi?
Jeśli wprowadzono inne polityki lub procedury z zakresu ochrony danych osobowych, podaj ich nazwy.
- g. Czy osoby przetwarzające dane zostały poinformowane o konieczności stosowania dokumentów wskazanych w poprzednim punkcie?
Podaj, w jaki sposób.
- h. Czy wdrożono zasady wyboru podmiotu, któremu dalej powierza się dane?
Opisz krótko, jak wybierani są i weryfikowani subprocesorzy
- i. Czy wprowadzono zasady bezpiecznej pracy zdalnej/hybrydowej?
Podaj jakie.
- j. Czy wdrożono proces analizy ryzyka naruszenia praw lub wolności osób fizycznych?
Podaj ogólne zasady działania procesu.

2. Inwentaryzacja danych oraz Rejestr Kategorii Czynność Przetwarzania (RKCP)

- a. Czy dokonano inwentaryzacji danych osobowych poprzez np. przeprowadzenie audytu?
- b. Czy istnieje RKCP i czy jest on zgodny z art. 30 RODO?
Podaj treść zawartych w RKCP wpisów dotyczących MESKO S.A.

3. Naruszenie ochrony danych osobowych i jego zgłoszenie do MESKO S.A.

- a. Czy wdrożona została procedura zarządzania incydentami bezpieczeństwa i naruszeniami ochrony danych osobowych?
Załącz procedurę lub opisz zasady badania źródła incydentu oraz jego zgłaszania do MESKO S.A. (m.in. czas zgłoszenia po wykryciu zdarzenia).
- b. Czy prowadzony jest wewnętrzny rejestr incydentów bezpieczeństwa i naruszeń ochrony danych osobowych? (incydent poufności, integralności oraz dostępności danych)

4. Dalsze powierzenie i udostępnienie danych, których Administratorem jest MESKO S.A.

- a. Czy wprowadzano zasadę powiadamiania MESKO S.A. o dalszym powierzeniu jego danych osobowych?
Podaj, kto jest za to odpowiedzialny.
- b. Czy prowadzony jest rejestr umów podmiotów, którym dane są dalej powierzane?
Podaj podmioty, którym powierzasz dane, dla których MESKO S.A. jest Administratorem.
- c. Czy dane, których Administratorem jest MESKO S.A., są przekazywane do państwa trzeciego?
Jeżeli tak, to podaj nazwy państw.
- d. Czy dane MESKO S.A. są udostępniane innym podmiotom?
Jeżeli tak, to podaj jakim.

5. Środki ochrony danych adekwatne do ryzyka prywatności

- a. Czy w oparciu o analizę ryzyka wdrożono adekwatne środki organizacyjne i techniczne zapewniające odpowiedni poziom bezpieczeństwa dla poufności, integralności, dostępności i odporności systemów oraz usług?
Podaj stosowane organizacyjne i techniczne środki bezpieczeństwa.
- b. Czy stosowane są adekwatne do ryzyka techniczne środki zabezpieczeń, np. IDS, firewalle, monitoring sieci?
Podaj jakie.
- c. Czy stosowana jest pseudonimizacja lub/i szyfrowanie danych osobowych?
Jeżeli tak, podaj, jakie techniki/rozwiązania są stosowane dla danych MESKO S.A.
- d. Czy stosowane są zasady bezpieczeństwa fizycznego i środowiskowego?
Podaj jakie.
- e. Czy opracowano plan ciągłości działania dla utrzymania zdolności do szybkiego przywrócenia dostępności danych w razie incydentu fizycznego lub technicznego?
Podaj datę ostatniego testu planu ciągłości działania.
- f. Czy stosowane jest regularne testowanie i ocenianie skuteczności wdrożonych środków organizacyjnych i technicznych mających zapewnić odpowiedni poziom bezpieczeństwa przetwarzania?
Podaj, jak wygląda proces.

Osoba uczestnicząca w audycie po stronie Podmiotu Przetwarzającego:

.....

Data imię i nazwisko

Osoba zatwierdzająca audyt po stronie Administratora – MESKO S.A.:

.....

Data imię i nazwisko

Raport został zatwierdzony w dniu: