6. Procedura kontroli podmiotów przetwarzających

1. Administrator Danych dopuszcza, by dane osobowe, których jest administratorem w rozumieniu art. 4 pkt 7 RODO, były przetwarzane poza jego strukturami organizacyjnymi przez podmioty przetwarzające.
2. Przetwarzanie danych osobowych przez podmioty przetwarzające może się odbywać wyłącznie w określonym celu i zakresie, na mocy umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego.
3. Administrator Danych ma prawo kontroli podmiotów przetwarzających, którym powierzył przetwarzanie danych osobowych z punktu widzenia zgodności tego przetwarzania z:
   3.1. przepisami prawa,
   3.2. postanowieniami zawartej umowy powierzenia przetwarzania danych osobowych,
   3.3. wytycznymi i rekomendacjami organów nadzorczych oraz organów doradczych w zakresie ochrony danych i prywatności.
4. Kontrola, o której mowa w pkt 3 prowadzona jest w postaci audytu podmiotu przetwarzającego.
5. Szczegóły dotyczące audytu podmiotu przetwarzającego określa zawarta z tym podmiotem umowa powierzenia przetwarzania danych osobowych. W szczególności, dotyczy to postanowień w zakresie sposobu i terminu przekazywania podmiotowi przetwarzającemu informacji o terminie i zakresie audytu.
6. W sytuacji, gdy umowa powierzenia przetwarzania danych osobowych nie określa sposobu i terminu przekazywania podmiotowi przetwarzającemu informacji o terminie i zakresie audytu, kwestie te ustalane są z tym podmiotem w formie porozumienia przed przeprowadzeniem pierwszego audytu, z zastrzeżeniem, że poczynione ustalenia pozostają właściwe dla przyszłych audytów.
7. Decyzję o przeprowadzeniu audytu podmiotu przetwarzającego podejmuje Administrator Danych:
   7.1. samodzielnie,
   7.2. na podstawie złożonego wniosku o przeprowadzenie audytu.
8. Z wnioskiem o przeprowadzenie audytu podmiotu przetwarzającego może wystąpić IOD.
9. Wniosek o przeprowadzenie audytu podmiotu przetwarzającego składany jest do Administratora Danych, a następnie przekazywany IOD.
10. Wniosek o przeprowadzenia audytu podmiotu przetwarzającego zawiera co najmniej:
    10.1. nazwę oraz siedzibę podmiotu przetwarzającego,

10.2. uzasadnienie konieczności przeprowadzenia audytu.

11. Na podstawie otrzymanego wniosku, Administrator Danych podejmuje ostateczną decyzję o przeprowadzeniu audytu podmiotu przetwarzającego. Gdy jest to zasadne, przed podjęciem decyzji, Administrator Danych konsultuje się z IOD.

12. Administratora Danych przekazuje IOD ostateczną decyzję

13. Audyt podmiotu przetwarzającego realizowany jest przez IOD. Jeżeli jest to zasadne, IOD realizuje audyt przy współpracy z innymi osobami upoważnionymi przez Administratora Danych, których wiedza może mieć kluczowe znaczenie dla merytorycznej poprawności przeprowadzanego audytu.

14. Audyt podmiotu przetwarzającego realizowany jest:

14.1. w siedzibie podmiotu przetwarzającego,

14.2. w głównym miejscu przetwarzania powierzonych danych osobowych, lub

14.3. zdalnie.

15. IOD opracowuje harmonogram przeprowadzania audytu, który wskazuje w szczególności na:

15.1. termin audytu,

15.2. miejsce audytu,

15.3. zakres audytu,

15.4. osoby biorące udział w audycie.

16. IOD informuje podmiot o terminie, miejscu i zakresie audytu.

17. IOD przeprowadza audyt z wykorzystaniem formularza audytu, którego wzór znajduje się w niniejszym Załączniku.

18. Formularz audytu uzupełniany jest:

18.1. w przypadku audytu w siedzibie podmiotu przetwarzającego lub w głównym miejscu przetwarzania powierzonych danych osobowych – przez IOD oraz inne osoby realizujące audyt, o których mowa w pkt 13,

18.2. w przypadku audytu zdalnego – przez osoby upoważnione do tego przez podmiot przetwarzający.

19. Po przeprowadzonym audycie IOD sporządza Protokół poaudytowy, według wzoru znajdującego się w niniejszym Załączniku.

20. IOD przekazuje Protokół poaudytowy:

20.1. Administratorowi Danych,

20.2. podmiotowi przetwarzającemu.

21. Podmiot przetwarzający ma 7 dni na ustosunkowanie się do treści przedstawionego mu Protokołu poaudytowego, z zastrzeżeniem, że umowa powierzenia przetwarzania danych osobowych zawarta z tym podmiotem może określać inny termin.

22. Jeżeli w wyniku audytu stwierdzono niezgodność przetwarzania powierzonych danych osobowych z:

22.1. obowiązującymi przepisami prawa, lub

22.2. postanowieniami zawartej umowy powierzenia przetwarzania danych osobowych,

22.3. wytycznymi i rekomendacjami organów nadzorczych oraz organów doradczych w zakresie ochrony danych i prywatności,

Administrator Danych, na podstawie przedłożonego mu Protokołu poaudytowego, podejmuje ostateczną decyzję w zakresie dalszej współpracy z podmiotem przetwarzającym.

23. Formularz audytu podmiotu przetwarzającego jest stosowany przez Administratora Danych również w stosunku do podmiotów, z którymi Administrator Danych chce nawiązać współpracę tj. potencjalnych podmiotów przetwarzających. W odniesieniu do takich podmiotów, niniejszą Procedurę kontroli podmiotów przetwarzających stosuje się odpowiednio z wyłączeniem pkt 5-6

FORMULARZ AUDYTU PODMIOTU PRZETWARZAJĄCEGO	
Administrator Danych	**Nazwa:** **Siedziba:**
Podmiot przetwarzający	**Nazwa:** **Siedziba:**
Data i miejsce audytu **w przypadku audytu zdalnego należy wskazać datę uzupełnienia Formularza*	
Osoby reprezentujące podmiot przetwarzający biorące udział w audycie **w przypadku audytu zdalnego należy wskazać osoby odpowiedzialne za uzupełnienie Formularza*	1. *…(imię, nazwisko, stanowisko, dane kontaktowe)…* 2. *…(imię, nazwisko, stanowisko, dane kontaktowe)…* 3. *…(imię, nazwisko, stanowisko, dane kontaktowe)…*
Osoby reprezentujące Administratora Danych biorące udział w audycie **w przypadku audytu zdalnego należy wskazać osoby do których Formularz jest wysyłany*	1. *…(imię, nazwisko, stanowisko, dane kontaktowe)…* 2. *…(imię, nazwisko, stanowisko, dane kontaktowe)…* 3. *…(imię, nazwisko, stanowisko, dane kontaktowe)…*

Lp.	Obszar	Pytania pomocnicze	Stan faktyczny
1.	**Usługi świadczone na rzecz Administratora Danych**	1. Jaki jest rodzaj usług świadczonych przez podmiot przetwarzający, w związku z którymi dochodzi do powierzenia przetwarzania danych osobowych?	
2.	**Zakres przetwarzanych danych osobowych**	1. Kogo dane osobowe są przetwarzane?	
		2. Czy przetwarzane są dane osób poniżej 16 r.ż.?	
		3. Jakie kategorie danych osobowych są przetwarzane?	
		4. Czy przetwarzane są szczególne kategorie danych? (*jakie*)	
		5. Czy przetwarza się dane dotyczące wyroków skazujących i naruszeń prawa?	
3.	**Struktura organizacyjna**	1. Czy wyznaczono Inspektora Ochrony Danych? (*imię, nazwisko oraz dane kontaktowe*)	
		2. Jeżeli nie wyznaczono IOD, czy wyznaczono osobę o podobnym stanowisku, nadzorującą kwestie związane z ochroną danych osobowych? (*funkcja, imię, nazwisko oraz dane kontaktowe*) 3. Czy wyznaczono osobę odpowiedzialną za zabezpieczenia danych osobowych przetwarzanych za pomocą systemów informatycznych? (*imię, nazwisko, stanowisko oraz dane kontaktowe*)	
4.	**Polityki ochrony danych**	1. Jakie polityki w zakresie ochrony danych	

	osobowych	osobowych została wdrożona?	
		2. W jaki sposób polityki ochrony danych osobowych została wdrożona? (*np. formalnie zatwierdzone i wprowadzone w życie procedury dot. środków ochrony danych osobowych*)	
		3. Czy jest przeprowadzana regularna aktualizacja tej polityk ochrony danych osobowych?	
5.	**Audyt**	1. Czy wdrożono program audytowy obejmujący zgodność z regulacjami w zakresie ochrony danych osobowych?	
		2. Jeżeli tak, kto jest odpowiedzialny za przeprowadzanie audytów?	
		3. Jakie są metody przeprowadzania audytów, ich częstotliwość oraz zakres?	
6.	**Incydenty**	1. Czy wdrożono procedurę postępowania z incydentami z zakresu ochrony danych osobowych?	
		2. Czy osoby posiadające dostęp do powierzonych danych osobowych zostali przeszkoleni w zakresie zgłaszania incydentów z zakresu ochrony danych osobowych?	
		3. Czy w okresie ostatnich trzech lat miały miejsce incydenty z zakresu ochrony danych osobowych? (*rodzaj, ilość*)	

		4. Czy w okresie ostatnich trzech lat działalność podmiotu przetwarzającego była przedmiotem postępowania ze strony urzędów zajmujących się ochroną danych osobowych? (*rodzaj, ilość*)	
		5. Czy w okresie ostatnich trzech lat działalność podmiotu przetwarzającego była przedmiotem działań prawnych dotyczących zarzutów naruszenia prywatności lub ochrony danych osobowych? (*rodzaj, ilość*)	
		6. Czy w okresie ostatnich trzech lat podmiot przetwarzający zgłosił jakiekolwiek naruszenia bezpieczeństwa danych odpowiednim organom / urzędom (uwzględniając organy związane z ochroną danych osobowych) oraz / lub podmiotom zajmującym się ochroną danych osobowych?	
		7. Czy podmiot przetwarzający jest zdolny do powiadomienia Administratora Danych o jakimkolwiek naruszeniu bezpieczeństwa, które mogłoby mieć negatywne skutki dla ochrony powierzonych do przetwarzania danych osobowych oraz praw i wolności osób, których te dane dotyczą, bez opóźnienia, tj. w ciągu 24 godzin od chwili powzięcia informacji o naruszeniu?	
7.	**Osoby posiadające dostęp do**	1. Czy stosuje się politykę lub procedurę ograniczającą dostęp do powierzonych danych	

	powierzonych danych osobowych w strukturze podmiotu przetwarzającego	osobowych?	
		2. W jaki sposób podejmowane są decyzje o tym, kto powinien otrzymać dostęp do powierzonych danych osobowych i w jaki sposób jest to sprawdzane i potwierdzane?	
		3. Jaka jest forma współpracy z osobami posiadającymi dostęp do powierzonych danych osobowych? (*umowa o pracę, umowa cywilnoprawna, umowa o współpracy*)	
		4. Czy osoby posiadające dostęp do powierzonych danych osobowych odbywają szkolenia w zakresie przetwarzania i ochrony prywatności danych oraz zgodności z przepisami prawa w zakresie ochrony danych osobowych? (*forma szkoleń, częstotliwość*)	
		5. Czy osobom posiadającym dostęp do powierzonych danych osobowych nadawane są upoważnienia do przetwarzania danych osobowych?	
		6. Czy osoby posiadające dostęp do powierzonych danych osobowych składają oświadczenia o zachowaniu tych danych w poufności przez okres trwania współpracy jak i po jej zakończeniu?	
		7. Czy prowadzona jest ewidencja osób posiadających dostęp do powierzonych danych osobowych?	

		8. Czy w przypadku zakończenia współpracy z osobami posiadającymi dostęp do powierzonych danych osobowych, fizyczny i elektroniczny dostęp do powierzonych danych osobowych jest odbierany natychmiast po zakończeniu współpracy? (*sposób odbioru dostępu*)	
8.	**Forma przetwarzania powierzonych danych osobowych**	1. W jakiej formie przetwarzane są powierzone dane osobowe? (*papierowa, elektroniczna*)	
		2. Jeżeli dane osobowe przetwarzane są w formie elektronicznej, za pomocą systemów informatycznych, proszę podać nazwy tych systemów.	
9.	**Miejsce przetwarzania powierzonych danych osobowych**	1. W jakich lokalizacjach ma miejsce przetwarzanie powierzonych danych osobowych? (*dane osobowe przetwarzane na bieżąco, wersje archiwalne, kopie zapasowe*)	
		2. Czy jest prowadzona aktualna ewidencja dotycząca lokalizacji i przemieszczania sprzętu i nośników elektronicznych, które mogą zawierać powierzone dane osobowe?	
10.	**Podpowierzanie powierzonych danych osobowych**	1. Czy powierzone dane osobowe są podpowierzane innym podmiotom?	
		2. Jeżeli tak, jakim podmiotom i w jakim zakresie? (*nazwy podmiotów, zakres danych podpowierzanych poszczególnym podmiotom*)	

		3. Czy z podmiotami, którym podpowierza się dane osobowe zawarto umowę podpowierzenia?	
		4. Czy zawarta umowa podpowierzenia przewiduje nałożenie na podmiot, któremu dane są podpowierzane te same obowiązki ochrony danych jakie zostały nałożone na podmiot przetwarzający na mocy umowy powierzenia z Administratorem Danych?	
		5. Czy podmiot przetwarzający monitoruje lub dokonuje audytu zgodności przetwarzania podpowierzonych danych osobowych z przepisami prawa oraz postanowieniami zawartej umowy podpowierzenia przetwarzania danych osobowych? (*zakres, częstotliwość audytów, metody, odpowiedzialność*)	
		6. Czy w przypadku zakończenia współpracy z podmiotem, któremu dane są podpowierzane, fizyczny i elektroniczny dostęp do powierzonych danych osobowych jest odbierany natychmiast po zakończeniu współpracy? (*sposób odbioru dostępu*)	
11.	**Udostępnianie powierzonych danych osobowych**	1. Czy powierzone dane osobowe są udostępniane innym podmiotom? (*zakres udostępnianych danych, nazwy podmiotów*)	
		2. Jeżeli tak, jakim podmiotom i w jakim zakresie? (*nazwy podmiotów, zakres danych udostępnianych poszczególnym podmiotom*)	

12.	**Przekazywanie powierzonych danych osobowych do państw trzecich**	1. Czy powierzone dane osobowe są przekazywane do państw trzecich?	
		2. Jeżeli tak, do jakich państw trzecich, jakim podmiotom, w jakim zakresie i na jakiej podstawie? (*państwo trzecie, nazwy podmiotów, zakres przekazywanych danych poszczególnym podmiotom, podstawa prawna*)	
13.	**Zabezpieczenia fizyczne**	1. Jakie zabezpieczenia fizyczne wdrożono dla ochrony powierzonych danych osobowych? **Należy opisać wdrożone zabezpieczenia fizyczne, w szczególności to jak zostały zabezpieczone pomieszczenia, w których przetwarzane są powierzone dane osobowe (polityki i procedury dostępu do pomieszczeń, rodzaj drzwi, rodzaj zamków, formy kontroli dostępu, formy zabezpieczenia przed osobami z zewnątrz, monitoring, ochrona, alarm, etc.) oraz to jak przechowuje się nośniki, na których przetwarzane są powierzone dane osobowe (rodzaje szaf, dane osobowe w formie papierowej (rodzaj szaf, zabezpieczenia fizyczne komputerów, niszczarki do dokumentów, etc.)*	
14.	**Zabezpieczenia techniczne**	1. Jakie zabezpieczenia techniczne wdrożono dla ochrony powierzonych danych osobowych? **Należy opisać wdrożone zabezpieczenia techniczne, w szczególności jakie środki wdrożone zostały dla ograniczenia dostępu do powierzonych danych*	

		osobowych (kontrola dostępu poprzez ograniczanie uprawnień, indywidualny login i hasło, wymagania dotyczące złożoności hasła, okresowa kontrola uprawnień, etc.), jakie środki techniczne są stosowane do zapewnienia bezpieczeństwa systemu (antywirus, firewall, IPS, IDS, etc.), jakie środki wdrożone zostały dla zagwarantowania rozliczalności, poufności i integralności powierzonych danych osobowych	

.....

Data i podpis osoby wypełniającej Formularz

Wzór protokołu poaudytowego

PROTOKÓŁ POAUDYTOWY NR …/……

…….

miejscowość, data

1. Administrator Danych: ……

2. Podmiot przetwarzający: ……..

3. Data rozpoczęcia audytu: ……..……

4. Data zakończenia audytu: ……..……

5. Miejsce audytu: ……..……

6. Osoby prowadzące czynności audytowe (*imiona, nazwiska, stanowiska*):

……..

7. Osoby upoważnione przez podmiot przetwarzający do udzielania wyjaśnień w trakcie czynności audytowych (*imiona, nazwiska, stanowiska*):

……

8. Zakres audytu:

……

9. Wykaz czynności podjętych w toku audytu:

…….

10. Wnioski poaudytowe:

…….

Kluczowe wnioski:

……

Stwierdzone niezgodności przetwarzania powierzonych danych osobowych z obowiązującymi przepisami prawa:

……

Stwierdzone niezgodności przetwarzania powierzonych danych osobowych z postanowieniami zawartej umowy powierzenia przetwarzania danych osobowych:

……

Stwierdzone niezgodności przetwarzania powierzonych danych osobowych z wytycznymi i rekomendacjami organów nadzorczych oraz organów doradczych w zakresie ochrony danych i prywatności

……

Rekomendacje:

……

11. Załączniki:

1) Formularz audytu podmiotu przetwarzającego z dnia …/…/……..

……

Data i podpis Inspektora Ochrony Danych

Otrzymują:
1 x oryginał Administrator Danych
1 x kopia podmiot przetwarzający
1 x kopia Inspektor Ochrony Danych