Warszawa, 31 stycznia 2019 r.

Związek Firm Ochrony Danych Osobowych

ul. Polna 50/615,
00-644 Warszawa

Sz. P. Edyta Bielak-Jomaa

Prezes Urzędu Ochrony Danych Osobowych
Urząd Ochrony Danych Osobowych
ul. Stawki 2,
00-193 Warszawa

Szanowna Pani Prezes,

W imieniu Związku Firm Ochrony Danych Osobowych (ZFODO), zrzeszającego najdłużej działające na rynku firmy zajmujące się ochroną danych osobowych, załączam wspólnie wypracowane stanowisko odnośnie standardowych klauzul umownych w umowach powierzenia.

Naszą intencją jest ułatwienie zawierania umów powierzenia poprzez ujednolicenie terminologii i tworzenia zapisów możliwych do akceptacji przez obie Strony.

Załączam efekt naszej pracy w dwóch postaciach:

1) Przejrzysta tabela z wnioskami ogólnymi dla Regulatora,
2) Szczegółowa część (poniżej,) stanowiąca szersze odniesienie się do zagadnień wraz z uzasadnieniem stanowiska ZFODO,

Ufamy, że nasze doświadczenie będzie pomocne przy tworzeniu nowych, praktycznych rozwiązań.

Z poważaniem,

Przemysław Zegarek
Prezes Związku Firm Ochrony Danych Osobowych

Stanowisko Związku Firm Ochrony Danych Osobowych w sprawie standardowych klauzul umownych w zakresie umów powierzenia przetwarzania danych

1. Jak dokumentować polecenia administratora polecenia administratora dotyczące przetwarzania danych?

1. Ogólne rozporządzenie o ochronie danych osobowych (dalej również jako **„RODO"**) w art. 28 ust. 3 lit. a wskazuje, że podmiot przetwarzający może przetwarzać dane osobowe wyłącznie na udokumentowane polecenie administratora. Polecenie administratora dotyczy także przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej.

2. RODO nie określa jednoznacznie jaką formę ma przyjąć takie polecenie, aby było skuteczne. Wskazówką interpretacyjną jest słowo „udokumentowane" co oznacza, że musi być w pewien sposób weryfikowalne zarówno dla procesora jak i administratora oraz musi być wyrazem wypełnienia zasady rozliczalności.

3. Nie ma konieczności, aby już w trakcie tworzenia umowy powierzenia lub innego instrumentu prawnego wskazywać konkretne formy polecenia. Interpretacja wyżej wskazanego przepisu pozwala stwierdzić, że na tym etapie wystarczy ustanowienie generalnego obowiązku by działanie procesora odbywało się na wyraźne polecenie administratora. Model, który sprawdzi się w konkretnej sytuacji może wyklarować się dopiero w trakcie trwania współpracy.

4. Powyższe wskazuje, że ustawodawca unijny daje administratorowi i procesorowi sporą swobodę w kształtowaniu swoich relacji. Podstawą jest by wszelkie polecenia, które kieruje administrator do procesora były konsekwentnie dokumentowane. Tylko bowiem wtedy będzie możliwość określenia, czy dane polecenie zostało wydane, czy zostało wykonane prawidłowo i kto ewentualnie ponosi odpowiedzialność za działania niezgodne z przepisami o ochronie danych osobowych.

5. Dokument może mieć formę zarówno pisemną jak i elektroniczną. Dla przykładu **polecenie może być przekazane wiadomością mailową, przy pomocy specjalnej platformy internetowej, listem poleconym, kurierem**. Niewykluczone, że takie polecenie, w sytuacjach nagłych może zostać przekazane **ustnie**. Należałoby wówczas sporządzić notatkę z rozmowy i bezzwłocznie otrzymać pisemne potwierdzenie polecenia. Można także w umowie głównej z góry wskazać w jakim czasie, jakie czynności procesor ma obowiązek wykonywać. W tej sytuacji **treść polecenia determinują obowiązki wynikające z umowy**. Słuszne wydaje się także, przy większych organizacjach, ustalenie osoby/osób, które w imieniu administratora mają prawo wydawać wiążące polecenia, a w imieniu procesora takie polecenia przyjmować.

6. Podsumowując, w kwestii dokumentowania poleceń administratora należy w sposób rozsądny korzystać ze **swobody danej przez ustawodawcę unijnego**, mając na uwadze: rodzaj współpracy, podmiot, któremu dane się powierza, stopień zaufania do niego, ryzyko związane z przetwarzaniem danych osobowych oraz własne obowiązki wynikające z RODO, związane przede wszystkim z zasadą rozliczalności. Należy mieć na uwadze ponadto, że sposób dokumentowania poleceń może mieć istotny wpływ na realizację zobowiązania podmiotu przetwarzającego do niezwłocznego informowania administratora o tym, że wydane mu polecenie stanowi naruszenie RODO lub innych przepisów prawa.

2. Jak weryfikować zobowiązania do zachowania tajemnicy przez osoby upoważnione do przetwarzania danych?

1. Zgodnie z art. 28 ust. 3 lit. b Ogólnego rozporządzenia o ochronie danych, jednym z obligatoryjnych elementów umowy powierzenia przetwarzania danych osobowych jest zobowiązanie osób upoważnionych do przetwarzania danych osobowych do zachowania tajemnicy, chyba że podlegają one takiemu obowiązkowi z mocy przepisów ustawowych. Przepisy Ogólnego rozporządzania o ochronie danych nie wskazują jednak sposobu weryfikacji spełnienia przez podmiot przetwarzający tego obowiązku. W naszej ocenie kontrola spełnienia tego wymogu może odbyć się:

   a. **poprzez odebranie od osób** upoważnionych przez podmiot przetwarzający do przetwarzania danych osobowych, stosownych **oświadczeń o zachowaniu tajemnicy** (przy czym oświadczenia takie nie muszą dotyczyć konkretnej umowy - wystarczające jest jedno oświadczenie ogólne o zachowaniu w tajemnicy informacji dotyczących wszystkich umów powierzenia),

   b. **poprzez złożenie przez podmiot przetwarzający oświadczenia, o zobowiązaniu osób upoważnionych do przetwarzania danych osobowych z zachowaniem poufności.**

2. Dodatkowo weryfikacja spełnienie tego obowiązku przez podmiot przetwarzający może odbyć się w ramach uprawnienia administratora wynikającego z art. 28 ust. 3 lit. h) Ogólnego rozporządzenia o ochronie danych, czyli udostępnienia wszelkich informacji niezbędnych do wykazania spełnienia obowiązków ciążących na administratorze. Jednym z elementów realizacji prawa do kontroli może być weryfikacja, realizowana zarówno w formie audytów osobowych lub bezosobowych (np. ankiet bezpieczeństwa wypełnianych przez podmiot przetwarzający), czy stosowne oświadczenia o zachowaniu tajemnicy zostały złożone przez wszystkie osoby upoważnione do przetwarzania danych.

3. Jak precyzyjnie powinny być w umowie wskazane środki bezpieczeństwa wymagane na mocy art. 32 RODO?

1. Ogólne rozporządzenie o ochronie danych nazywane jest w doktrynie aktem „technologicznie obojętnym", co oznacza, że nie wskazuje, co do zasady, konkretnych środków zabezpieczenia danych osobowych (zarówno fizycznych, jak i technicznych), jakie powinni stosować administratorzy oraz podmioty przetwarzające. Stąd można wywnioskować, iż wolą ustawodawcy unijnego było **uniknięcie nadmiernej precyzji** w zakresie doboru środków zapewniających odpowiedni poziom bezpieczeństwa przetwarzania danych osobowych i nałożenie ciężaru analizy ryzyka i wyboru sposobów zabezpieczenia danych na administratorów albo podmioty przetwarzające.
2. W praktyce tworzenia i negocjowania umów powierzenia spotkać można dwa stanowiska:
    a. obowiązki podmiotu przetwarzającego, w zakresie zabezpieczenia danych, wskazywane są **w sposób ogólny** np. poprzez odniesienie do regulacji art. 32 RODO, który wymienia **przykładowe formy zabezpieczeń**, jakie można zastosować;
    b. **precyzyjne wskazanie** (poprzez wyliczenie) środków bezpieczeństwa, jakie powinien zastosować podmiot przetwarzający w ramach powierzenia przetwarzania danych osobowych np. poprzez **listę wymaganych zabezpieczeń** stanowiącą załącznik do umowy powierzenia przetwarzania danych osobowych.
3. Stosowanie wobec każdego podmiotu przetwarzającego, z którego korzysta administrator danych, jednolitego wzoru umowy powierzenia przetwarzania danych osobowych, której załącznikiem byłaby lista środków bezpieczeństwa, rodzi ryzyko braku adekwatności wymaganych zabezpieczeń do specyfiki i branży, w której funkcjonuje podmiot przetwarzający, a także do kategorii danych oraz operacji, które w danej sytuacji są przedmiotem powierzenia. Rodzi to zatem obawę, iż przyjęcie przez Prezesa Urzędu Ochrony Danych Osobowych precyzyjnego katalogu sposobów zabezpieczenia danych, **nie spełniałoby kryterium klauzul umownych standardowych** tj. dających się do zastosowania w zdecydowanej większości przypadków powierzenia przetwarzania danych osobowych.
4. Obecnie mamy do czynienia z bardzo szybkim tempem rozwoju technologii, a co za tym idzie również sposobów zabezpieczenia, w szczególności środków technicznych. Przepisy prawa często nie są w stanie nadążyć, w naszej ocenie, za postępem w zakresie zagrożeń oraz ich przeciwdziałaniu. Stąd też przyjęcie, w omawianym zakresie, przez organ nadzoru standardowych klauzul umownych, który wymieniałyby konkretne środki bezpieczeństwa (przykładowo: jaki

rodzaj szyfrowania, powinien być stosowany zgodnie z art. 32 ust. 1 lit. a) RODO) rodzi ryzyko **szybkiej dezaktualizacji**. To z kolei prowadziłoby do konieczności regularnych i częstych nowelizacji katalogu zabezpieczeń, co może powodować stan niepewności prawnej.

5. Przepisy Ogólnego rozporządzenia o ochronie danych nakładają na administratorów i podmioty przetwarzające ciężar doboru odpowiednich środków zabezpieczenia oraz przeprowadzenia w tym zakresie oceny ryzyka. Stąd też organ nadzoru **nie powinien zbyt mocno ingerować w sferę autonomii decyzyjnej** administratorów lub podmiotów przetwarzających w zakresie doboru środków zabezpieczenia danych. Należy również wskazać, że administrator danych posiada prawo weryfikacji stosowanych przez podmiot przetwarzający zabezpieczeń zarówno na etapie negocjacji warunków umowy powierzenia, jak i w trakcie jej obowiązywania (art. 28 ust. 3 lit. h) RODO).

6. Organ nadzoru posiada, w sposób pośredni, możliwość wpływania na katalog zabezpieczeń danych dla określonej branży. Istnieją bowiem dwa mechanizmy prawne, które mogą doprowadzić do wypracowania pewnych jednolitych standardów i wymogów w omawianym zakresie, a należą do nich w myśl art. 32 ust. 3 RODO: zatwierdzone kodeksy postępowania oraz zatwierdzone mechanizmy certyfikacji. Dostrzegamy użyteczność wskazania w sposób precyzyjny zabezpieczeń, jakie wdrożyć powinni procesorzy, jednakże uważamy, iż nie powinno się to odbywać na najwyższym poziomie ogólności tj. jako standardowa klauzula umowna w rozumieniu art. 28 ust. 8 RODO, lecz w **zatwierdzonych kodeksach postępowania** lub **mechanizmach certyfikacji** tzn. na wyższym poziomie szczegółowości, z uwzględnieniem specyfiki działalności podmiotów przetwarzających w danej branży.

7. Z uwagi na powyższe rekomendujemy przyjęcie, jako standardowych klauzul umownych, w zakresie wskazania środków bezpieczeństwa, **sformułowań na wysokim poziomie ogólności**, pozostawiając jednocześnie swobodę doboru środków administratorowi i podmiotowi przetwarzającemu w ramach swobody kontraktowania.

4. Jak skutecznie wywiązywać się z obowiązków związanych z realizacją żądań osoby, której dane dotyczą?

1. Na podstawie art. 28 ust. 3 lit. e Ogólnego rozporządzenia o ochronie danych umowa powierzenia przetwarzania lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający *„biorąc pod uwagę charakter przetwarzania, w miarę możliwości **pomaga administratorowi** poprzez odpowiednie środki techniczne i organizacyjne wywiązać się*

z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III;"

2. Postanowienia umowne, które mają na celu realizację wskazanego wyżej obowiązku powinny przede wszystkim **precyzować tryb i sposób** w jaki podmiot przetwarzający (procesor) będzie wspierał administratora w zakresie realizacji żądań pochodzących od osób wykonujących prawa określone w art. 15-22 RODO. Postanowienia takie powinny określać, w szczególności :

   a. **termin**, w jakim podmiot przetwarzający powinien udzielić administratorowi informacji, z tym zastrzeżeniem, że termin ten powinien być **adekwatny do potrzeby** realizacji żądań osób, których dane dotyczą, **uwzględniający terminy określone w art. 12 ust. 3 RODO oraz uzasadnione interesy** zarówno administratora jak i podmiotu przetwarzającego,

   b. **zakres** udzielonej „*pomocy*", który powinien polegać na **udostępnianiu wszelkich danych i informacji** jakie będą niezbędne dla administratora, dla realizacji celu jakim jest odpowiadanie na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III. W określonych sytuacjach, stosownie do charakteru i zakresu powierzenia, umowa może także regulować **sposób,** w jaki procesor będzie realizował prawa osób (działając w tym zakresie w imieniu administratora), a w szczególności sposób i formy kontaktu z osobami składającymi żądania, bądź wyłączać możliwość udzielania przez podmiot przetwarzający pomocy w formie bezpośredniego kontaktu z osobami, których dane dotyczą. Postanowienia umowy, gdy jest to konieczne, mogą precyzować, czy i w jaki sposób oraz w jakim zakresie podmiot przetwarzający może działać w tym zakresie w imieniu administratora.

   c. **formę** przekazywania danych i informacji, która może być adekwatna do potrzeb realizacji praw osób, których dane dotyczą np. **pisemna**, **elektroniczna** (w szczególności w postaci przesłania danych pocztą email np. kopii obrazu wyświetlonego na ekranie urządzenia, kopii zapisów rejestrów systemu informatycznego (logi systemowe), umożliwienie dostępu do systemu informatycznego) lub **ustna** (ustne udzielenie informacji).

   d. **osoby uprawione do kontaktu** tj. osoby - po stronie administratora **uprawione do kierowania żądań** o udzielenie „*pomocy*" oraz osoby - po stronie podmiotu przetwarzającego uprawnione do przyjmowania takich żądań i udzielania odpowiedzi,

3. Zgodnie z treścią wskazanego wyżej art. 28 ust. 3 lit. e RODO pomoc podmiotu przetwarzającego ma odbywać się poprzez zastosowanie odpowiednich środków technicznych i organizacyjnych. Nie można więc wykluczyć, że w pewnych przypadkach – w interesie administratora, będzie, aby w umowie zobowiązał on procesora do zapewnienie **określonych – minimalnych wymogów**

dotyczących stosowania odpowiednich środków technicznych i organizacyjnych np. służących do wykazania rozliczalności wykonywanych przez procesora czynności.

4. Co niezwykle istotne, doprecyzowanie trybu i sposobu wspierania administratora przez procesora musi uwzględniać określone okoliczności faktyczne, które – zgodnie z cytowanym przepisem wyznaczane są przez „*charakter powierzenia*" oraz możliwości podmiotu przetwarzającego. **Postanowienia umowne regulujące wsparcie procesora na rzecz administratora powinny być zatem dostosowane do charakteru współpracy między nimi.**

5. Przykładowo, inne powinny być wymagania dla globalnej firmy IT świadczącej usługę bieżącego wsparcia systemu informatycznego banku, a inne dla jednoosobowej agencji marketingowej, która przyjęła jednorazowe zlecenie przeprowadzenia konkursu.

6. W każdym jednak przypadku, postanowienia umowne powinny być tak sformułowane, aby zapewnić możliwie **jak najwyższy poziom współdziałania** podmiotu przetwarzającego z administratorem. Głównym celem regulacji z art. 28 ust. 3 lit. e RODO jest bowiem **zapewnienie mechanizmów służących skutecznej realizacji praw osób, których dane dotyczą zgodnie z wymogami określonymi w rozdziale III RODO.**

5. Jak realizować obowiązek udostępnienia informacji niezbędnych do wykazania spełnienia obowiązków ciążących na administratorze (m.in. art. 28, 32-36 RODO)?

1. Na wstępie należy wskazać, iż obowiązek udostępnienia informacji przez podmiot przetwarzający, niezbędnych do wykazania spełnienia obowiązków ciążących na administratorze, wiąże się nierozerwalnie z obowiązkiem postępowania, zarówno przez administratora, jak i procesora, w zgodzie z zasadą rozliczalności, którą statuuje art. 5 ust. 2 RODO.

2. W pierwszej kolejności podkreślamy, że udostępnienie informacji przez procesora, na wysokim poziomie ogólności, powinno przybrać **formę oświadczenia podmiotu przetwarzającego**, iż spełnia wymogi z art. 28 oraz 32-36 RODO, a także **zobowiązanie tego podmiotu do dalszego utrzymywania takiego stanu zgodności**. Oświadczenie i zobowiązanie podmiotu przetwarzającego powinno stanowić jedno z postanowień umowy powierzenia. Tym samym procesor, zgadzając się na warunki umowy powierzenia, jednocześnie oświadczy administratorowi, iż znane mu są wymogi przetwarzania wskazane w wymogi z art. 28 oraz 32-36 RODO oraz zobowiąże się, iż przetwarzając powierzone dane w przyszłości, spełniać będzie wymogi powołanych wyżej przepisów.

3. Oświadczenia, o których mowa w pkt 2, administrator powinien móc **weryfikować**. Trudno bowiem sądzić, iż oświadczenie, nawet w postaci zapisu umownego, będzie wystarczającym

środkiem do wykazania przez podmiot przetwarzający wobec administratora, iż spełnia wymogi przewidziane w art. 28 oraz 32-36 RODO. Wskazujemy zatem, iż zasadnym byłoby przygotowanie przez Prezesa Urzędu Ochrony Danych Osobowych **standardowej klauzuli umownej w zakresie możliwości weryfikacji procesora**, pod kątem spełniania wymogów wyżej wskazanych przepisów, w zakresie kontroli podmiotu przetwarzającego (w zależności od rodzaju działalności i stopnia ryzyka: w postaci audytów osobowych lub bezosobowych, np. wypełniania ankiet bezpieczeństwa).

4. Wydaje się również, że mechanizmem, który może wspomóc w realizacji obowiązków procesora udostępnienia informacji, o których mowa w pytaniu, jest **udokumentowane polecenie administratora**, o którym mowa w art. 28 ust. 3 lit. a RODO. Standardowa klauzula umowna mogłaby przewidywać zatem obowiązek udostępnienia pewnych informacji przez podmiot przetwarzający na polecenie administratora danych, przy zachowaniu warunków określonych w art. 28 ust. 3 akapit drugi RODO.

5. Jak zapewniać zgodność działań innego podmiotu przetwarzającego z postanowieniami umowy zawartej z administratorem?

1. W codziennym obrocie gospodarczym bardzo często dochodzi do sytuacji, w których podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego (podprocesora). Procesor wykonuje konkretne czynności przetwarzania w imieniu administratora danych, korzystając przy tym z usług podprocesora. A zatem administrator danych korzystając z usług procesora powinien mieć pewność, że procesor skorzysta z usług innego podmiotu przetwarzającego, który da gwarancje przetwarzaniach danych zgodnego z prawem. W jaki sposób w takiej sytuacji zabezpieczyć interesy administratora?

2. Zgodnie z treścią **art. 28 ust. 4 Ogólnego rozporządzenia o ochronie danych,** jeśli mamy do czynienia z sytuacją wykonania w imieniu administratora konkretnych czynności przetwarzania przez inny podmiot przetwarzający – **te same obowiązki ochrony danych między administratorem, a podmiotem przetwarzającym należy nałożyć (umownie lub na mocy innego aktu prawnego) na inny podmiot przetwarzający.** Te obowiązki zostały szczegółowo określone w art. 28 ust. 3 RODO, w szczególności jest to obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych zgodnych z RODO.

3. **Procesor przed administratorem jest odpowiedzialny za działania i zaniechania podprocesora jak za działania i zaniechania własne.** Aby zatem zabezpieczyć interesy

administratora i procesora należy do umowy wprowadzić odpowiednie postanowienia umowne – wymagane przez art. 28 ust. 3 RODO.

4. Z punktu widzenia administratora najlepszym rozwiązaniem będzie sytuacja, w której administrator danych zapewni sobie prawo do kontroli podprocesora. Taka kontrola umożliwi wykazanie, że podprocesor spełnia wymogi określone w przepisach obowiązującego prawa, a także umowie między administratorem i procesorem, a także procesorem i podprocesorem. Oczywiście kontrola może nastąpić na skutek działań organu nadzoru, gdy jest związana z powierzeniem danych podprocesorowi. Kontrola może być realizowana w postaci audytu osobowego lub bezosobowego (np. w postaci ankiety bezpieczeństwa).

5. **Postanowienia dotyczące kontroli realizowanej w postaci <u>audytu</u> powinny zapewnić, że:**

   a. w trakcie kontroli nie może dojść do naruszenia tajemnicy przedsiębiorstwa podprocesora, natomiast administrator będzie mógł żądać wykazania przez podprocesora, że spełnia wymogi określone w RODO i umowie między procesorem i podprocesorem,

   b. kontrola może wymagać udostępnienia dokumentacji, pomieszczeń i infrastruktury technicznej w zakresie niezbędnym do przeprowadzenia kontroli, niemniej tych informacji można żądać wyłącznie, jeśli mają związek z powierzeniem danych podprocesorowi,

   c. kontrolerzy są zobowiązani do zachowania w tajemnicy wszelkich informacji pozyskanych w trakcie kontroli,

   d. kontrola powinna zostać zapowiedziana, chyba że sytuacja wymaga niezwłocznego działania, np. na skutek naruszenia związanego z przetwarzaniem danych osobowych – wtedy może odbyć się niezwłocznie,

   e. po przeprowadzonej kontroli przygotowany jest protokół, który powinien zawierać ewentualne uchybienia. Podprocesor powinien mieć możliwość ustosunkowania się i usunięcia ewentualnych naruszeń.

6. **Postanowienia dotyczące kontroli realizowanej w postaci wypełnienia <u>ankiety bezpieczeństwa</u> powinny zapewnić, że:**

   a. ankieta bezpieczeństwa odnosi się do wszystkich istotnych obowiązków podprocesora, wynikających z zawartej umowy powierzenia oraz przepisów RODO,

   b. adekwatny termin przekazania wszystkich informacji żądanych w ankiecie, zbieżny z terminem realizacji obowiązku, o którym mowa w art. 28 ust. 3 lit. e i f RODO,

   c. formę przeprowadzenia ankiety, pisemną lub elektroniczną,

d. zobowiązanie podprocesora do realizacji zaleceń pokontrolnych wystosowanych w wyniku analizy wypełnionej ankiety bezpieczeństwa.

7. W przypadku, gdyby naruszeń nie dało się usunąć, może być to podstawa **do żądania przez administratora zamiany podprocesora przez procesora na inny podmiot**. W przypadku niemożności zastąpienia podprocesora innym podmiotem, administrator może zyskać prawo do wypowiedzenia umowy z procesorem, który nie jest w stanie realizować umowy o współpracę.

8. Jako element zabezpieczenia interesów administratora, należałoby rozważyć obowiązek dostarczania mu **wyciągu z umowy zawartej między procesorem a podprocesorem**. W wyciągu musiałyby się znaleźć obligatoryjne obowiązki, wskazane w art. 28 RODO, zawarte w umowie między administratorem i procesorem. Brak dostarczenia takiego dokumentu skutkowałby brakiem zgody na współpracę procesora z podprocesorem, co mogłoby także prowadzić do wypowiedzenia umowy administratora z procesorem.

9. Z punktu widzenia administratora, w niektórych przypadkach powierzenia przetwarzania danych osobowych, uzasadnione może być także nałożenie na procesora obowiązku sprawowania kontroli nad podprocesorem, przeprowadzania audytów, obowiązku informowania administratora o wynikach takich kontroli lub audytu, w tym sygnalizowania nieprawidłowości w zakresie działań niezgodnych z postanowieniami umowy zawartej z administratorem.

6. Określanie w umowie powierzenia przetwarzania danych osobowych: przedmiotu i czasu trwania przetwarzania, charakteru i celu przetwarzania, rodzaju danych osobowych oraz kategorii osób, których dane dotyczą.

1. Ogólne rozporządzenie o ochronie danych określa w art. 28 ust. 3 jakie obligatoryjne elementy powinna zawierać umowa powierzenia przetwarzania danych osobowych. Zgodnie z powoływanym artykułem, dokument powinien określać m.in.: przedmiot przetwarzania, czas trwania przetwarzania, charakter przetwarzania, cel przetwarzania, rodzaj danych osobowych, kategorie osób, których dane dotyczą.

2. Prawidłowa interpretacja wskazanych w pkt 1 elementów, jest kluczowa z punktu widzenia uznania zawartej umowy powierzenia przetwarzania danych osobowych za spełniającą wymogi Ogólnego rozporządzenia o ochronie danych.

3. Praktyka pokazuje, że różne podmioty, niezależnie od tego czy pełnią rolę administratora danych czy też podmiotu przetwarzającego, inaczej interpretują obligatoryjne elementy umowy powierzenia przetwarzania danych osobowych. Różniącą się od siebie interpretację tych elementów prezentują również dostępne komentarze do Ogólnego rozporządzenia o ochronie

danych tj. *Ogólne rozporządzenie o ochronie danych. Komentarz*, Bielak-Jomaa Edyta (red.), Lubasz Dominik (red.) oraz *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Litwiński Paweł (red.), Barta Paweł, Kawecki Maciej.

4. Brak jednolitej interpretacji prowadzi to niejednokrotnie do przedłużania się procesu negocjacji, a w skrajnych przypadkach do niepodpisania umowy z uwagi na brak osiągnięcia porozumienia w tym zakresie. Inną konsekwencją braku jednoznacznego wskazania sposobu rozumienia postanowień art. 28 ust. 3 Ogólnego rozporządzenia o ochronie danych, jest zawieranie przez ten sam podmiot umów powierzenia przetwarzania danych osobowych o różnej treści (tj. zawierających różne interpretacje przedmiotowych elementów).

5. Z uwagi na powyższe, postuluje się o **jednoznaczne wskazanie sposobu interpretacji elementów obligatoryjnych umowy powierzenia przetwarzania danych osobowych**.

6. Mając na uwadze wieloletnie doświadczenie oraz praktykę przy zawieraniu oraz realizacji umów powierzenia przetwarzania danych osobowych rekomenduje się następujące sposoby interpretacji:

   a. **przedmiot przetwarzania**, jako wskazanie:

      - **działań / usług w związku z którymi dochodzi do powierzenia** przetwarzania danych osobowych, w szczególności poprzez **odwołanie się do głównej umowy o współpracy** zawartej między administratorem a podmiotem przetwarzającym,
      - **zakresu powierzanych danych** poprzez określenie **poszczególnych kategorii**, (np. imię, nazwisko, email, numer telefonu, adres zamieszkania, etc.), z możliwością modyfikacji tego zakresu poprzez polecenie administratora, bez wymogu aneksowania umowy, ale z zachowaniem zasady rozliczalności,
      - **operacji przetwarzania**, do których dokonywania uprawniony jest podmiot przetwarzający, niezbędnych do realizacji głównej umowy o współpracy, ze wskazaniem w miarę możliwości, funkcjonalnego opisu tych operacji, a także ze wskazaniem operacji, do których w szczególności uprawniony jest podmiot przetwarzający, poprzez dokonanie wyboru **z katalogu operacji wskazanych w art. 4 pkt 2) Ogólnego rozporządzenia o ochronie danych**, z możliwością modyfikacji tego katalogu poprzez polecenie administratora, bez wymogu aneksowania umowy, ale z zachowaniem zasady rozliczalności,
      - **formy przetwarzania danych** osobowych, tj. czy przetwarzanie będzie odbywało się w **formie papierowej** czy też **przy wykorzystaniu systemów** informatycznych,

b. **<u>czas trwania przetwarzania</u>**, jako odesłanie do **czasu trwania głównej umowy o współpracy** w związku, z którą dochodzi do powierzenia przetwarzania danych osobowych, z uwzględnieniem czasu przewidzianego na zwrot / usunięcie danych przez podmiot przetwarzający po zakończeniu współpracy,

c. **<u>charakter przetwarzania</u>**, jako określenie, czy przetwarzanie powierzonych danych osobowych będzie miało charakter **cykliczny** (tj. stały przez cały okres trwania umowy, np. przy outsourcingu takich usług jak kardy i płace), **sporadyczny** (tj. wypadkowy, np. przy outsourcingu nadzoru nad infrastrukturą IT, gdzie przy poszczególnych pracach może dojść do dostępu do danych osobowych) czy też **jednorazowy** (przy umowach na jednorazowe działania / usługi, np. jednorazowa kampania marketingowa),

d. **<u>cel przetwarzania</u>** jako wskazanie ze względu **na jaką główną umowę o współpracy powierzenie przetwarzania danych osobowych stało się konieczne** (np. umożliwienie prawidłowej realizacji umowy o świadczenie usług kadr i płac),

e. **<u>rodzaj danych osobowych</u>**, jako wskazanie, czy powierzenie przetwarzania obejmuje tzw. **szczególne kategorie danych** i/lub **dane osobowe dotyczące wyroków skazujących i czynów zabronionych**, tj. dane, o których mowa w art. 9 i/lub art. 10 Ogólnego rozporządzenia o ochronie danych,

f. **<u>kategorie osób, których dane dotyczą</u>**, jako wskazanie **określonej grupy pomiotów danych** (np. potencjalni pracownicy, pracownicy, klienci, kontrahenci, etc.), z możliwością modyfikacji tego zakresu poprzez polecenie administratora, bez wymogu aneksowania umowy, ale z zachowaniem zasady rozliczalności.