Przykład klauzul umownych dotyczących powierzenia przetwarzania

Poniższy przykład klauzul dotyczących powierzenia przetwarzania został przygotowany w oczekiwaniu na przyjęcie klauzul , o których mowa w art. 28 punkt 8 rozporządzenia. Poniższe klauzule mogą zostać włączone do Państwa umów. Muszą one zostać dostosowane oraz doprecyzowane mając na uwadze konkretną operację powierzenia przetwarzania. Należy zauważyć, że niniejsze klauzule nie stanowią same w sobie umowy powierzenia przetwarzania.

[…], z siedzibą w […] oraz reprezentowany przez […]
(zwany dalej „administratorem danych”]
z jednej strony,

ORAZ

[…], z siedzibą w […] oraz reprezentowany przez […] (odtąd „podmiot przetwarzający”)
z drugiej,

Przedmiot

Celem niniejszych klauzul jest określenie warunków na jakich podmiot przetwarzający może w imieniu administratora danych przetwarzać dane osobowe, w zakresie zdefiniowanym poniżej.

W ramach swoich umów strony zobowiązują się do przestrzegania mających zastosowanie przepisów w obszarze ochrony danych w tym w szczególności Rozporządzenia nr 2016/679 Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 r. stosowanego od dnia 25 maja 2018 r. (dalej *europejskie rozporządzenie ds. ochron danych*).

I. Opis operacji przetwarzania będących przedmiotem powierzenia

Podmiot przetwarzający zostaje upoważniony do przetwarzania w imieniu administratora danych, danych osobowych koniecznych do dostarczenia następujących usług […]

Operacje przetwarzania danych mają następujący charakter […]
Dane są przetwarzane do następujących celów […]
Przetwarzane są następujące kategorie danych […]
Przetwarzane są dane następujących kategorii osób, których dane dotyczą […].

W celu wykonania niniejszej umowy administrator danych udziela podmiotowi przetwarzającemu następujących, niezbędnych informacji […].

II. Okres trwania umowy

Niniejsza umowa obowiązuje od dnia […] na okres […]

III. Obowiązki podmiotu przetwarzającego wobec administratora danych

Podmiot przetwarzający zobowiązuje się do:

1. przetwarzania danych **wyłącznie w celu/celach,** dla których zostały one powierzone;

2. przetwarzania danych **zgodnie z udokumentowanymi instrukcjami** administratora danych załączonymi w formie aneksu do niniejszej umowy. Jeżeli zdaniem podmiotu przetwarzającego instrukcja taka stanowi naruszenie rozporządzenia w sprawie ochrony danych lub jakichkolwiek innych przepisów Unii Europejskiej lub państw członkowskich mających wpływ na ochronę danych, **informuje o tym natychmiast** administratora danych. Ponadto jeżeli podmiot przetwarzający jest zobowiązany do dokonywania transferu danych do państw trzecich lub organizacji międzynarodowej, zgodnie z prawem Unii lub prawem państwa członkowskiego, któremu podlega, musi poinformować administratora danych o tym zobowiązaniu prawnym przed rozpoczęciem przetwarzania, chyba że ww. prawo zabrania udzielenia takiej informacji ze względu na ważne względy interesu publicznego;

3. zapewnienia **poufności** danych osobowych przetwarzanych w ramach niniejszej umowy;

4. zapewnienia **aby osoby upoważnione do przetwarzania danych osobowych** na mocy niniejszej umowy:
   - zobowiązały się do zapewnienia **poufności** lub podlegały obowiązkowi prawnemu zachowania poufności;
   - odbyły odpowiednie **szkolenie** w obszarze ochrony danych osobowych;

5. uwzględniania przy wykorzystywaniu swoich narzędzi, produktów, oprogramowania lub usług zasad **ochrony danych w fazie projektowania** oraz **domyślnej ochrony danych**;

6. **Powierzenie przetwarzania**

   Proszę wybrać jedną z dwóch możliwości:

   ***Opcja A** (ogólne upoważnienie)*

   Podmiot przetwarzający może skorzystać z innego podmiotu przetwarzającego […] (dalej **podwykonawca przetwarzania**) w celu wykonania określonych czynności przetwarzania. W takim wypadku, informuje on uprzednio na piśmie administratora danych o wszystkich przewidywanych zmianach dotyczących dodania lub zastąpienia podwykonawcy przetwarzania. Informacja ta musi jasno wskazywać czynności, które mają być dalej powierzone, tożsamość oraz dane kontaktowe podwykonawcy przetwarzania oraz datę podpisania umowy. Administrator danych dysponuje terminem […] od momentu otrzymania ww. informacji na przedstawienie swojego sprzeciwu. Podzlecenie może nastąpić jedynie, jeżeli administrator danych nie zgłosi swojego sprzeciwu w ww. terminie.

Opcja B *(konkretne upoważnienie)*

Podmiot przetwarzający może skorzystać z innego podmiotu przetwarzającego […] (dalej ***podwykonawca przetwarzania***) w celu wykonania następujących operacji przetwarzania […]. W przypadku zatrudnienia innych podwykonawców przetwarzania, podmiot przetwarzający musi uzyskać uprzednią pisemną, konkretną zgodę od administratora danych.

Niezależnie od wybranej opcji *(upoważnienie ogólne lub konkretne)*

Podwykonawca przetwarzania jest zobowiązany do przestrzegania obowiązków ustanowionych w niniejszej umowie w imieniu oraz zgodnie z instrukcjami administratora danych. Obowiązkiem początkowego podmiotu przetwarzającego jest zapewnienie, że podwykonawca przetwarzania posiada równorzędne, wystarczające środki w odniesieniu do wdrożenia środków organizacyjnych i technicznych w taki sposób aby przetwarzanie odpowiadało wymogom europejskiego rozporządzenia w sprawie ochrony danych. Jeżeli podwykonawca przetwarzania nie wykonuje swoich obowiązków w obszarze ochrony danych, początkowy podmiot przetwarzający ponosi pełną odpowiedzialność przed administratorem danych za wykonanie przez inny podmiot przetwarzający swoich obowiązków.

7. **Prawo do informacji osób, których dane dotyczą**

Wybór jednej z dwóch opcji

Opcja A
Obowiązkiem administratora jest przekazanie informacji osobom, których dane dotyczą o operacjach przetwarzania w momencie zebrania danych.

Opcja B
Podmiot przetwarzający, w momencie zbierania danych, musi przekazać osobom, których dane dotyczą informacje o operacjach przetwarzania, które realizuje. Treść oraz forma informacji musi zostać uzgodniona z administratorem danych przed zebraniem danych.

8. **Wykonywanie praw przez osoby, których dane dotyczą**
W miarę możliwości podmiot przetwarzający pomaga administratorowi danych w wypełnianiu jego obowiązku podejmowania działań związanych z wykonywaniem praw osób, których dane dotyczą: prawa dostępu, poprawiania, usunięcia oraz wyrażenia sprzeciwu, prawa do ograniczenia przetwarzania, prawa do przenoszenia danych, prawa do nie podleganiu zautomatyzowanej decyzji indywidualnej (co obejmuje profilowanie).

Proszę wybrać jedną z dwóch opcji

Opcja A
Jeżeli osoba, której dane dotyczą zwraca się z wnioskiem o skorzystanie ze swoich praw do podmiotu przetwarzającego, podmiot przetwarzający musi przesłać ten wniosek pocztą elektroniczną na adres […] (wskazać kontakt po stronie administratora danych).

Opcja B
Podmiot przetwarzający musi odpowiedzieć w imieniu administratora danych oraz w terminie przewidzianym w europejskim rozporządzeniu w sprawie ochrony danych na wnioski osób, których dane dotyczą w sytuacji wykonywania ich praw, w odniesieniu do danych będących przedmiotem powierzenia na podstawie niniejszej umowy.

9. **Naruszenie bezpieczeństwa ochrony danych osobowych**
Podmiot przetwarzający informuje administratora danych o wszystkich naruszeniach danych osobowych w terminie maksymalnie […] godzin po powzięciu wiedzy o tym naruszeniu, przy użyciu następujących środków […]. Notyfikacji tej towarzyszy pełna dokumentacja pozwalająca administratorowi danych, jeśli to konieczne, na notyfikację tego naruszenia właściwemu organowi nadzorczemu.

Możliwa opcja

Po uzyskaniu zgody administratora danych, podmiot przetwarzający notyfikuje odpowiedniemu organowi nadzorczemu (CNIL) w imieniu administratora danych naruszenie ochrony danych w jak najszybszym terminie oraz, jeśli to możliwe, najpóźniej w ciągu 72 godzin od powzięcia wiedzy o tym naruszeniu, chyba że jest mało prawdopodobne, by naruszenie to mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.

Notyfikacja obejmuje przynajmniej:

- opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazuje kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
- imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- opis możliwych konsekwencji naruszenia ochrony danych osobowych;
- opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.

Po uzyskaniu zgody administratora danych podmiot przetwarzający informuje, w imieniu administratora danych, o naruszeniu ochrony danych osobowych osobę, której dane dotyczą w jak najszybszym terminie, chyba że jest mało prawdopodobne, by naruszenie to mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.

Informacja dla osoby, której dane dotyczą opisuje w prostych słowach charakter naruszenia bezpieczeństwa danych osobowych oraz obejmuje co najmniej:

- opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazanie kategorii i przybliżonej liczby osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
- imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- opis możliwych konsekwencji naruszenia ochrony danych osobowych;
- opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

10. **Pomoc podmiotu przetwarzającego administratorowi danych w przestrzeganiu przez niego swoich obowiązków**

Podmiot przetwarzający pomaga administratorowi danych w przeprowadzeniu przez niego oceny wpływu na ochronę danych.

Podmiot przetwarzający pomaga administratorowi danych w przeprowadzeniu uprzednich konsultacji z organem nadzorczym.

11. **Środki bezpieczeństwa**

Podmiot przetwarzający zobowiązuje się wprowadzić następujące środki bezpieczeństwa:

[Należy opisać środki techniczne i organizacyjne zapewniające poziom bezpieczeństwa dostosowany do ryzyka obejmujący, m.in.

- pseudonimizację oraz szyfrowanie danych osobowych;
- zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Podmiot przetwarzający zobowiązuje się wprowadzić środki bezpieczeństwa przewidziane przez *[kodeks postępowania, certyfikaty].*

[Tam gdzie art. 32 rozporządzenia europejskiego o ochronie danych osobowych przewiduje wdrożenie środków bezpieczeństwa przez administratora danych oraz podmiot przetwarzający, zaleca się precyzyjne określenie obowiązków każdej ze stron w odniesieniu do środków, które należy wdrożyć] .

12. **Usunięcie danych**

Po zakończeniu świadczenia usług związanych z przetwarzaniem podmiot przetwarzający zobowiązuje się do:

Wyboru przez Strony:

- zniszczenia wszystkich danych osobowych,
- zwrócenia wszystkich danych osobowych administratorowi danych, lub
- zwrócenia danych osobowych podmiotowi przetwarzającemu wyznaczonemu przez administratora danych.

Zwrotowi danych musi towarzyszyć zniszczenie wszystkich istniejących kopii w systemach informatycznych podmiotu przetwarzającego. Po zniszczeniu danych podmiot przetwarzający musi na piśmie przedstawić dowód zniszczenia.

13. **Inspektor ochrony danych**

Podmiot przetwarzający informuje administratora danych **o nazwisku oraz danych kontaktowych inspektora ochrony danych**, jeżeli zgodnie z art. 37 rozporządzenia o ochronie danych został on powołany.

14. **Rejestr kategorii czynności przetwarzania danych**

Podmiot przetwarzający deklaruje **prowadzenie w formie pisemnej rejestru** wszystkich kategorii czynności przetwarzania wykonywanych w imieniu administratora danych, obejmującego:

- Nazwę oraz dane kontaktowe administratora danych w imieniu którego działa podmiot przetwarzający, potencjalnie inne podmioty przetwarzający oraz, jeżeli dotyczy, inspektora ochrony danych;
- Kategorie operacji przetwarzania wykonywanych w imieniu administratora danych;
- Jeżeli dotyczy, przekazanie danych osobowych do państw trzecich lub organizacji międzynarodowej, co obejmuje wskazanie tych państw trzecich lub organizacji międzynarodowej oraz, w przypadku przekazania danych zgodnie z art. 49 ust. Ustęp 1 punkt 2 rozporządzenia w sprawie ochrony danych dokumenty potwierdzające istnienie odpowiednich gwarancji;
- Na ile to wykonalne, ogólny opis środków technicznych oraz organizacyjnych, które obejmują, wedle potrzeby, następujące elementy:
    - pseudonimizację i szyfrowanie danych osobowych;
    - zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
    - zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
    - regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

15. **Dokumentacja**

Podmiot przetwarzający udostępnia administratorowi danych **dokumentację niezbędną do wykazania spełnienia wszystkich swoich obowiązków** oraz w celu umożliwienia audytu, co obejmuje inspekcje przeprowadzane przez administratora danych lub innego upoważnionego przez niego audytora, a także wspieranie audytu.

IV. Obowiązki administratora danych wobec podmiotu przetwarzającego

Administrator danych zobowiązuje się, że:

1. dostarczy podmiotowi przetwarzającemu dane określone w punkcie II niniejszych klauzul;
2. będzie dokumentował w formie pisemnej wszystkie instrukcje dotyczące przetwarzania dla podmiotu przetwarzającego;
3. zapewni, przed oraz w trakcie trwania przetwarzania, poszanowanie obowiązków przewidzianych w europejskim rozporządzeniu w sprawie ochrony danych przez podmiot przetwarzający;
4. będzie nadzorował przetwarzanie co obejmuje wykonywanie audytów oraz inspekcji wobec podmiotu przetwarzającego.