Dofinansowane przez Unię Europejską

sieć splot wartości

WZÓR

Umowa powierzenia przetwarzania danych osobowych

dla organizacji pozarządowych

Opracowanie: Fundacja LegisLab

Stan prawny na dzień: wrzesień 2026 r.

Z komentarzem [FL1]: JAK KORZYSTAĆ Z WZORU. (1) Przed zawarciem umowy usuń tę kartę tytułową, stopkę z oznaczeniami projektu oraz wszystkie komentarze. (2) Uzupełnij pola w nawiasach kwadratowych [ ] – wskazówki w nawiasach usuń. (3) Postanowienia oznaczone [opcjonalnie] pozostaw albo usuń, zależnie od rodzaju powierzanych danych i skali przetwarzania. (4) Wzór jest przygotowany z perspektywy organizacji jako administratora danych, który powierza dane zewnętrznemu podmiotowi, i chroni przede wszystkim interes administratora.

Wzór ma charakter pomocniczy i nie stanowi porady prawnej. Przed zawarciem umowy należy dostosować jej treść do rzeczywistego zakresu powierzenia danych osobowych w danej organizacji.

Grant realizowany ze środków Unii Europejskiej w ramach projektu SPLOT WARTOŚCI 2.0

Program finansowany jest przez Unię Europejską. Wyrażone opinie i poglądy są wyłącznie poglądami autora (autorów) i niekoniecznie odzwierciedlają poglądy Unii Europejskiej lub Komisji Europejskiej. Ani Unia Europejska, ani organ przyznający finansowanie nie mogą ponosić za nie odpowiedzialności.

Umowa powierzenia
przetwarzania danych osobowych

zawarta w dniu …… w …….. pomiędzy:

[nazwa organizacji] z siedzibą w [miejscowość], [adres], wpisaną do Krajowego Rejestru Sądowego pod numerem KRS [●], NIP [●], REGON [●],
reprezentowaną przez:
[imię i nazwisko, funkcja – zgodnie ze sposobem reprezentacji ujawnionym w KRS]

zwaną dalej **Administratorem**, a

[firma albo imię i nazwisko] z siedzibą (adresem wykonywania działalności) w [miejscowość], [adres], wpisaną do [Krajowego Rejestru Sądowego pod numerem KRS [●] / Centralnej Ewidencji i Informacji o Działalności Gospodarczej], NIP [●], REGON [●], reprezentowaną przez: [imię i nazwisko, funkcja],
zwaną dalej **Podmiotem przetwarzającym,** zaś łącznie „**Stronami**”,

o następującej treści:

PREAMBUŁA

A. Niniejsza umowa powierzenia przetwarzania danych osobowych, zwana dalej „Umową Powierzenia”, zawarta jest w związku z umową […….] z dnia […….], zwaną dalej „Umową Główną” oraz w celu wykonywania Umowy Głównej.

B. Na podstawie Umowy Głównej Podmiot przetwarzający zobowiązał się do świadczenia usług […….] na rzecz Administratora.

C. W celu wykonania Umowy Głównej niezbędne jest przetwarzanie danych osobowych przez Podmiot przetwarzający. W związku z tym konieczne jest zawarcie niniejszej Umowy Powierzenia.

§ 1

Oświadczenia Stron

1. Przetwarzanie danych osobowych z tytułu Umowy Głównej odbywać się będzie w zgodzie i w oparciu o Rozporządzenie 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) zwanego dalej „RODO”.
2. W trybie art. 28 ust. 3 RODO, Administrator powierza Podmiotowi przetwarzającemu do przetwarzania dane osobowe, które zgromadził zgodnie z obowiązującymi przepisami prawa, a Podmiot przetwarzający zobowiązuje się do ich przetwarzania zgodnie z Umową Główną i Umową Powierzenia.

Z komentarzem [FL2]: KIEDY POTRZEBNA JEST UMOWA POWIERZENIA? Gdy zewnętrzny podmiot przetwarza dane osobowe w imieniu organizacji i na jej polecenie (art. 28 RODO), np.: biuro rachunkowe lub osoba prowadząca księgowość, firma utrzymująca stronę internetową lub pocztę, informatyk z dostępem do komputerów i kont, dostawca systemu zapisów lub bazy kontaktów (CRM), zewnętrzna osoba koordynująca projekt na podstawie umowy cywilnoprawnej. Umowa NIE jest potrzebna, gdy podmiot przetwarza dane we własnym imieniu i we własnych celach – np. bank, operator pocztowy, ZUS, urząd skarbowy, co do zasady kancelaria prawna. Z dużymi dostawcami usług chmurowych (np. Google, Microsoft, Canva, MailerLite) nie podpisuje się indywidualnej umowy – organizacja akceptuje ich standardową umowę powierzenia (DPA). Warto zachować jej kopię w dokumentacji ochrony danych i odnotować dostawcę w rejestrze czynności przetwarzania.

Z komentarzem [FL3]: Dane organizacji wpisz zgodnie z aktualnym odpisem z KRS. Umowę podpisują osoby uprawnione do reprezentacji zgodnie z KRS i statutem (często wymagane są podpisy dwóch członków zarządu) albo pełnomocnik – wtedy wskaż podstawę umocowania. Stowarzyszenie zwykłe wskazuje numer w ewidencji prowadzonej przez starostę i przedstawiciela albo zarząd; koło gospodyń wiejskich – numer w rejestrze kół gospodyń wiejskich.

Z komentarzem [FL4]: Jeżeli Podmiotem przetwarzającym jest osoba prowadząca jednoosobową działalność gospodarczą (np. księgowa), wpisz imię i nazwisko, firmę z CEIDG, adres wykonywania działalności, NIP i REGON, a fragment o reprezentacji usuń. Dla spółki wpisz numer KRS i osoby uprawnione do reprezentacji. Dostosuj końcówki („wpisanym”, „zwanym”) do rodzaju podmiotu.

Z komentarzem [FL5]: Opisz usługę wynikającą z Umowy Głównej, np. „prowadzenia ksiąg rachunkowych i obsługi kadrowo-płacowej” albo „utrzymania i serwisu strony internetowej oraz poczty elektronicznej”. Jeżeli usługa jest świadczona bez pisemnej umowy (np. na podstawie zlecenia mailowego), w pkt A wskaż datę i sposób jej zawarcia.

3. Podmiot przetwarzający oświadcza również, że wszystkim osobom działającym z jego upoważnienia, które mają dostęp do powierzonych danych osobowych, nadane zostały upoważnienia do przetwarzania danych osobowych, o których mowa w art. 29 i art. 32 ust. 4 RODO oraz że osoby te zostały zapoznane z przepisami o ochronie danych osobowych oraz z odpowiedzialnością za ich nieprzestrzeganie, zobowiązały się do ich przestrzegania oraz do bezterminowego zachowania w tajemnicy przetwarzanych danych osobowych i sposobów ich zabezpieczenia.

4. Z tytułu wykonywania Umowy Powierzenia Podmiotowi przetwarzającemu nie przysługuje wynagrodzenie odrębne od wynagrodzenia określonego w Umowie Głównej.

5. Osobami do kontaktu w sprawach związanych z wykonywaniem Umowy Powierzenia są: po stronie Administratora – [imię i nazwisko, adres e-mail, numer telefonu], a po stronie Podmiotu przetwarzającego – [imię i nazwisko, adres e-mail, numer telefonu]. Jeżeli Strona wyznaczyła inspektora ochrony danych, kontakt z nim jest możliwy pod adresem: [●].

§ 2

Cel, zakres, miejsce przetwarzania powierzonych danych osobowych

1. Administrator powierza Podmiotowi przetwarzającemu przetwarzanie danych osobowych jedynie w celu prawidłowego wykonywania Umowy Głównej.

2. Podmiot przetwarzający zobowiązuje się do przetwarzania powierzonych danych osobowych wyłącznie w celach związanych z realizacją Umowy Głównej i wyłącznie w zakresie, jaki jest niezbędny do realizacji tych celów, w odniesieniu do następujących kategorii osób, których dane dotyczą: [np. członkowie organizacji, wolontariusze, uczestnicy zajęć i wydarzeń – w tym osoby małoletnie oraz ich rodzice lub opiekunowie prawni, darczyńcy, pracownicy i współpracownicy, osoby korzystające ze wsparcia organizacji]. Powierzenie obejmuje następujące kategorie danych osobowych:

   a. dane zwykłe: [np. imię, nazwisko, adres zamieszkania, adres e-mail, numer telefonu, data urodzenia, numer rachunku bankowego; numer PESEL – wyłącznie gdy jest to niezbędne],

   b. dane szczególnych kategorii (art. 9 ust. 1 RODO): [np. dane dotyczące stanu zdrowia – jeżeli są powierzane; w przeciwnym razie wpisać „nie dotyczy"],

   c. dane dotyczące wyroków skazujących oraz czynów zabronionych (art. 10 RODO): [np. informacje uzyskane z Rejestru Sprawców Przestępstw na Tle Seksualnym lub z Krajowego Rejestru Karnego w ramach weryfikacji osób dopuszczanych do pracy lub działalności z małoletnimi – jeżeli są powierzane; w przeciwnym razie wpisać „nie dotyczy"].

3. Charakter przetwarzania obejmuje: [np. prowadzenie ksiąg rachunkowych i rozliczeń płacowych / utrzymanie strony internetowej i skrzynek poczty elektronicznej / obsługę systemu zapisów lub wysyłki newslettera]. Przetwarzanie odbywa się [w formie papierowej / w formie elektronicznej / w obu tych formach], w szczególności z wykorzystaniem następujących systemów informatycznych lub usług: [nazwa systemu lub usługi].

Z komentarzem [FL6]: Oświadczenia Podmiotu przetwarzającego (§ 1, § 3 ust. 7, § 5) dokumentują, że organizacja wybrała podmiot zapewniający wystarczające gwarancje ochrony danych (art. 28 ust. 1 RODO). W razie kontroli Prezesa UODO organizacja musi wykazać tę staranność (zasada rozliczalności – art. 5 ust. 2 RODO), dlatego warto przechowywać korespondencję i dokumenty otrzymane od Podmiotu przetwarzającego razem z umową.

Z komentarzem [FL7]: Wskaż wyłącznie te kategorie osób i danych, które faktycznie są przekazywane Podmiotowi przetwarzającemu (zasada minimalizacji – art. 5 ust. 1 lit. c RODO). Przykład dla biura rachunkowego: pracownicy, zleceniobiorcy, członkowie zarządu; imię, nazwisko, PESEL, adres, numer rachunku bankowego, dane o wynagrodzeniu, a z danych szczególnych kategorii – wyłącznie informacje o niezdolności do pracy. Przykład dla firmy hostingowej: osoby korzystające z formularza kontaktowego i subskrybenci newslettera; imię, adres e-mail, adres IP.

Z komentarzem [FL8]: Dotyczy organizacji pracujących z dziećmi, które przed dopuszczeniem osoby do pracy lub działalności z małoletnimi weryfikują ją w Rejestrze Sprawców Przestępstw na Tle Seksualnym i w KRK (art. 21 ustawy o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich). Takie dane powierzaj tylko wtedy, gdy jest to konieczne (np. zewnętrznemu biuru kadrowemu), i uwzględnij to w standardach ochrony małoletnich organizacji.

4. Podmiot przetwarzający nie jest uprawniony do przetwarzania danych w innym zakresie niż wskazany powyżej, ani do ich dalszego powierzania inaczej niż na zasadach określonych w § 3 ust. 13–15.
5. Na wniosek Administratora Podmiot przetwarzający wskaże miejsca, w których przetwarza powierzone dane.
6. Przez przetwarzanie danych osobowych rozumie się wszelkie operacje wykonywane na powierzonych danych osobowych w zakresie niezbędnym do wykonania Umowy Głównej, takie 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.

§ 3

Zasady przetwarzania danych osobowych

1. Strony zobowiązują się wykonywać zobowiązania wynikające z niniejszej Umowy Powierzenia z najwyższą starannością zawodową w celu zabezpieczenia prawnego, organizacyjnego i technicznego interesów Stron w zakresie przetwarzania powierzonych danych osobowych.
2. Podmiot przetwarzający zobowiązuje się zastosować środki techniczne i organizacyjne mające na celu należyte, odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, zabezpieczenie powierzonych do przetwarzania danych osobowych, w szczególności zabezpieczyć je przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa, oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
3. Podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora. Dotyczy to również przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, chyba że obowiązek przetwarzania nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega; w takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny. Za udokumentowane polecenie uważa się w szczególności niniejszą Umowę Powierzenia oraz polecenia przekazane przez Administratora w formie dokumentowej, w tym wiadomością e-mail.
4. Podmiot przetwarzający niezwłocznie informuje Administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie RODO lub innych przepisów Unii lub państwa członkowskiego o ochronie danych. Do czasu wyjaśnienia wątpliwości Podmiot przetwarzający może wstrzymać się z wykonaniem takiego polecenia.
5. Podmiot przetwarzający nie przekazuje powierzonych danych osobowych do państwa trzeciego (poza Europejski Obszar Gospodarczy) ani do organizacji międzynarodowej, również za pośrednictwem dalszego podmiotu przetwarzającego, bez uprzedniej zgody Administratora wyrażonej w formie dokumentowej. Przekazanie może nastąpić wyłącznie przy spełnieniu warunków określonych w rozdziale V RODO.

6. Zakazuje się wykorzystywania danych do celów własnych Podmiotu przetwarzającego, profilowania lub marketingu. Zakazuje się także łączenia powierzonych danych z danymi przetwarzanymi przez Podmiot przetwarzający we własnym imieniu lub na rzecz innych podmiotów. Podmiot przetwarzający wdraża zasadę minimalizacji danych i privacy by design/by default.

7. Podmiot przetwarzający oświadcza, że dysponuje zasobami, doświadczeniem, wiedzą fachową i wykwalifikowanym personelem, które umożliwiają mu prawidłowe wykonanie Umowy Powierzenia oraz wdrożenie odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO.

8. 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. Podmiot przetwarzający bez zbędnej zwłoki, nie później niż w 3 dni robocze, przekazuje Administratorowi każde żądanie osoby oraz nie odpowiada na nie bez uprzedniego upoważnienia, chyba że bezwzględnie wymagają tego przepisy prawa.

9. Podmiot przetwarzający, uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga Administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO.

10. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora, nie później niż w ciągu 24 godzin od wykrycia, o każdym naruszeniu ochrony danych osobowych powierzonych przez Administratora, niezależnie od jego charakteru i skali. Zgłoszenie powinno zawierać w szczególności: opis charakteru naruszenia, w tym – o ile to możliwe – kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie; opis możliwych konsekwencji naruszenia; opis środków zastosowanych lub proponowanych w celu zaradzenia naruszeniu, w tym w celu zminimalizowania jego ewentualnych negatywnych skutków, oraz dane kontaktowe osoby, od której można uzyskać więcej informacji. Jeżeli informacji nie można udzielić w tym samym czasie, Podmiot przetwarzający udziela ich sukcesywnie, bez zbędnej zwłoki. Zgłoszenie przesyłane jest mailowo na adres [adres e-mail Administratora], a informacja o jego przesłaniu przekazywana jest też telefonicznie na numer [numer telefonu Administratora]. Podmiot przetwarzający nie zgłasza naruszenia organowi nadzorczemu ani nie zawiadamia o nim osób, których dane dotyczą, bez polecenia Administratora.

Z komentarzem [FL9]: Administrator ma 72 godziny od stwierdzenia naruszenia na zgłoszenie go Prezesowi UODO (art. 33 RODO) – im szybciej Podmiot przetwarzający przekaże informacje, tym więcej czasu na ocenę ryzyka. Po otrzymaniu zgłoszenia postępuj zgodnie z procedurą reagowania na naruszenia z polityki ochrony danych organizacji i odnotuj zdarzenie w rejestrze naruszeń – także wtedy, gdy nie zgłaszasz go do UODO.

11. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem, w terminie 30 dni od dnia ich zakończenia, w zależności od decyzji Administratora danych usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych. Podmiot przetwarzający przygotowuje protokół usunięcia (zniszczenia) danych i przekazuje go na pierwsze żądanie Administratora.

12. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszej Umowie Powierzenia oraz umożliwia Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich, na zasadach określonych w § 7.

13. Podmiot przetwarzający może korzystać z usług innego podmiotu przetwarzającego (dalszego podmiotu przetwarzającego) wyłącznie na podstawie ogólnej zgody Administratora, na zasadach określonych w niniejszym ustępie oraz w ust. 14 i 15. Administrator wyraża zgodę na korzystanie przez Podmiot przetwarzający z następujących dalszych podmiotów przetwarzających: [nazwa, adres siedziby, zakres powierzonych czynności i miejsce przetwarzania – np. dostawca programu księgowego w chmurze, dostawca usług hostingowych; jeżeli nie dotyczy – wpisać „brak"].

14. Podmiot przetwarzający informuje Administratora w formie dokumentowej o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia dalszych podmiotów przetwarzających co najmniej 14 dni przed planowaną zmianą, wskazując dane tego podmiotu, zakres powierzanych mu czynności i miejsce przetwarzania. W tym terminie Administrator może wyrazić sprzeciw wobec takiej zmiany; brak sprzeciwu oznacza zgodę na zmianę. W razie sprzeciwu Podmiot przetwarzający nie może powierzyć danych temu podmiotowi, a jeżeli dalsze wykonywanie Umowy Głównej bez tej zmiany nie jest możliwe, Administrator może rozwiązać Umowę Powierzenia oraz Umowę Główną bez zachowania okresu wypowiedzenia.

15. Podmiot przetwarzający nakłada na dalszy podmiot przetwarzający – w drodze umowy lub innego aktu prawnego, o którym mowa w art. 28 ust. 4 RODO – te same obowiązki ochrony danych, jakie spoczywają na nim na podstawie Umowy Powierzenia, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom RODO. Jeżeli dalszy podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie tych obowiązków spoczywa na Podmiocie przetwarzającym.

16. Obowiązek zachowania poufności, o którym mowa w niniejszej Umowie Powierzenia, obowiązuje także po zakończeniu obowiązywania Umowy Głównej i Umowy Powierzenia, bez względu na przyczynę jej rozwiązania, i dotyczy zarówno Podmiotu przetwarzającego, jak i osób przez niego zatrudnionych lub zaangażowanych do przetwarzania danych.

Z komentarzem [FL10]: Zapytaj Podmiot przetwarzający przed podpisaniem umowy, z jakich podmiotów korzysta (np. biuro rachunkowe korzysta zwykle z programu księgowego w chmurze i z usług hostingowych), i wpisz je tutaj. Model ogólnej zgody z prawem sprzeciwu (art. 28 ust. 2 RODO) nie wymaga aneksu przy każdej zmianie, ale oznacza, że brak reakcji na powiadomienie w ciągu 14 dni jest równoznaczny ze zgodą. Powiadomienia przechowuj razem z umową.

§ 4

Odpowiedzialność Stron

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią Umowy Powierzenia, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym, w innych celach niż wynikają z niniejszej Umowy Powierzenia.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w Umowie Powierzenia, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w

szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora.

3. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem, jeśli nie dopełnił obowiązków, które nakłada niniejsza Umowa Powierzenia, lub gdy działał poza zgodnymi z prawem instrukcjami Administratora lub wbrew tym instrukcjom.
4. Podmiot przetwarzający ma obowiązek współdziałania z Administratorem na jego żądanie w zakresie ustalenia przyczyn szkody wyrządzonej osobie, której dane dotyczą, jak również zapewnia, że ten obowiązek będzie wypełniać dalszy podmiot przetwarzający.
5. W przypadku, gdy Podmiot przetwarzający naruszy przepisy RODO, inne powszechnie obowiązujące przepisy, postanowienia Umowy Powierzenia, w następstwie czego w stosunku do Administratora zostanie wydane jakiekolwiek orzeczenie, w tym organ nadzorczy nałoży na Administratora dodatkowe obowiązki lub karę – Podmiot przetwarzający zobowiązany jest pokryć poniesione z tego tytułu koszty lub naprawić szkodę w części, za którą ponosi odpowiedzialność.
6. [opcjonalnie] Podmiot przetwarzający utrzymuje ważne ubezpieczenie odpowiedzialności cywilnej [oraz ubezpieczenie od ryzyk cybernetycznych] adekwatne do skali i rodzaju przetwarzania.

Z komentarzem [FL11]: Ubezpieczenie OC mają m.in. biura rachunkowe – w ich przypadku jest obowiązkowe (art. 76h ustawy o rachunkowości). Ubezpieczenie od ryzyk cybernetycznych jest rzadkie u małych podmiotów – wymagaj go tylko przy dużej skali przetwarzania lub danych szczególnie wrażliwych. W pozostałych przypadkach ustęp można usunąć.

§ 5
Weryfikacja i zapewnienia Podmiotu przetwarzającego

1. Podmiot przetwarzający oświadcza, że posiada wdrożone odpowiednie środki techniczne i organizacyjne, o których mowa w art. 32 RODO, zapewniające stopień bezpieczeństwa danych osobowych odpowiadający ryzyku ich przetwarzania, a także zapewnia zgodność przetwarzania z przepisami RODO oraz innymi przepisami prawa powszechnie obowiązującego.
2. W szczególności Podmiot przetwarzający oświadcza, że:
    a. wdrożył i stosuje wewnętrzne procedury ochrony danych osobowych,
    b. posiada dokumentację wewnętrzną w zakresie przetwarzania danych, w tym: politykę ochrony danych osobowych, procedurę reagowania na naruszenia ochrony danych osobowych i politykę bezpieczeństwa systemów informatycznych,
    c. prowadzi rejestr kategorii czynności przetwarzania, o którym mowa w art. 30 ust. 2 RODO,
    d. dysponuje aktualną ewidencją upoważnień do przetwarzania danych oraz stosuje zasadę ograniczonego dostępu,
    e. zobowiązuje wszystkie osoby upoważnione do przetwarzania danych do zachowania poufności w zakresie przetwarzanych danych, zarówno w trakcie, jak i po zakończeniu współpracy,
    f. zapewnia, że jego pracownicy i współpracownicy zostali przeszkoleni z zakresu ochrony danych osobowych i znają swoje obowiązki,
    g. wdrożył środki techniczne chroniące dane przed nieuprawnionym dostępem, w tym kontrolę dostępu (indywidualne konta użytkowników, silne hasła lub uwierzytelnianie wieloskładnikowe), zabezpieczenia antywirusowe i zapory sieciowe oraz szyfrowanie przenośnych nośników danych i urządzeń mobilnych, na których przetwarzane są powierzone dane;
    h. utrzymuje aktualność oprogramowania oraz stosuje proces zarządzania poprawkami bezpieczeństwa;

Z komentarzem [FL12]: Katalog w lit. a–i jest proporcjonalny także dla małych podmiotów, np. jednoosobowego biura rachunkowego. Lit. j oznaczoną [opcjonalnie] pozostaw przy powierzaniu danych szczególnych kategorii, danych osób małoletnich lub danych dużej liczby osób. Lit. c: zwolnienie z prowadzenia rejestru dla podmiotów zatrudniających mniej niż 250 osób (art. 30 ust. 5 RODO) nie obejmuje przetwarzania, które nie ma charakteru sporadycznego – podmiot świadczący stałe usługi z reguły musi prowadzić rejestr.

i. regularnie tworzy kopie zapasowe powierzonych danych i okresowo sprawdza możliwość ich odtworzenia;
j. [opcjonalnie – zalecane przy powierzaniu danych szczególnych kategorii, danych osób małoletnich lub danych dużej liczby osób:] przeprowadza testy odtwarzania kopii zapasowych nie rzadziej niż raz na pół roku, utrzymuje plany ciągłości działania (BCP) i odtwarzania po awarii (DRP), stosuje systemy monitorowania dostępu do danych oraz prowadzi okresowe testy świadomości personelu (np. symulacje ataków phishingowych).

3. Podmiot przetwarzający zobowiązuje się do przekazania Administratorowi, na jego żądanie zgłoszone w formie dokumentowej, aktualnych kopii powyższych dokumentów lub ich fragmentów (w zakresie niezbędnym do wykazania zgodności z RODO), w terminie nie dłuższym niż 7 dni roboczych od dnia otrzymania żądania.
4. Podmiot przetwarzający niezwłocznie informuje Administratora o istotnych zmianach mogących wpływać na bezpieczeństwo, w tym zmianie lokalizacji przetwarzania, wykorzystywanej infrastruktury, zmianach właścicielskich lub zmianie kontroli nad Podmiotem przetwarzającym, a także o negatywnych wynikach audytów bezpieczeństwa.

§ 6
Czas obowiązywania umowy

Niniejsza Umowa Powierzenia obowiązuje od dnia jej zawarcia przez czas trwania Umowy Głównej, o której mowa w pkt A Preambuły. Obowiązki określone w § 3 ust. 11 (usunięcie lub zwrot danych) i ust. 16 (poufność) wiążą Podmiot przetwarzający również po rozwiązaniu lub wygaśnięciu Umowy Powierzenia.

§ 7

Uprawnienia kontrolne Administratora

1. Administrator lub upoważniony przez niego audytor zewnętrzny ma prawo do przeprowadzenia kontroli przestrzegania przez podmiot przetwarzający zasad przetwarzania danych osobowych, o których mowa w Umowie Powierzenia oraz w obowiązujących przepisach prawa, w szczególności w sposób opisany w § 5 ust. 3 Umowy Powierzenia, a także poprzez żądanie udzielenia informacji dotyczących przetwarzania przez podmiot przetwarzający, stosowanych środków technicznych i organizacyjnych, aby przetwarzanie toczyło się zgodnie z prawem lub dokonywania kontroli w miejscach, w których są przetwarzane powierzone dane osobowe, po wcześniejszym uzgodnieniu terminu przez Strony na 5 dni przed planowaną kontrolą. Podmiot przetwarzający dokona niezbędnych czynności w celu umożliwienia wykonania tego uprawnienia przez Administratora.
2. Podmiot przetwarzający jest zobowiązany do zastosowania się do zaleceń Administratora dotyczących zasad przetwarzania powierzonych danych osobowych oraz dotyczących poprawy zabezpieczenia danych osobowych, sporządzonych w wyniku kontroli przeprowadzonych przez Administratora lub upoważnionego przez niego audytora w terminie wyznaczonym przez Administratora, nie dłuższym niż 14 dni roboczych, o ile Strony nie ustalą inaczej.

§ 8

Rozwiązanie umowy

Administrator może rozwiązać niniejszą Umowę Powierzenia ze skutkiem natychmiastowym, gdy Podmiot przetwarzający:

a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;

b) przetwarza dane osobowe w sposób niezgodny z Umową Powierzenia;

c) powierzył przetwarzanie danych osobowych dalszemu podmiotowi przetwarzającemu bez zgody Administratora lub pomimo jego sprzeciwu.

Rozwiązanie Umowy Powierzenia z przyczyn wskazanych powyżej uprawnia Administratora do rozwiązania Umowy Głównej bez zachowania okresu wypowiedzenia.

§ 9

Postanowienia końcowe

1. Zmiany niniejszej Umowy Powierzenia wymagają formy pisemnej lub elektronicznej pod rygorem nieważności, z zastrzeżeniem ust. 2.
2. Zmiana danych kontaktowych, o których mowa w § 1 ust. 5 i § 3 ust. 10, oraz zmiana wykazu dalszych podmiotów przetwarzających dokonana w trybie § 3 ust. 14 nie stanowią zmiany Umowy Powierzenia i wymagają jedynie zachowania formy dokumentowej.
3. W zakresie nieuregulowanym niniejszą Umową Powierzenia zastosowanie mają przepisy RODO, ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych oraz Kodeksu cywilnego.
4. W przypadku, gdy niniejsza Umowa Powierzenia odwołuje się do przepisów prawa, oznacza to również inne przepisy dotyczące ochrony danych osobowych, a także wszelkie nowelizacje, jakie wejdą w życie po dniu zawarcia Umowy Powierzenia, jak również akty prawne, które zastąpią wskazane ustawy i rozporządzenia.
5. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy miejscowo dla siedziby Administratora.
6. Umowę Powierzenia sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron, albo – w przypadku zawarcia w formie elektronicznej – w postaci dokumentu elektronicznego opatrzonego kwalifikowanymi podpisami elektronicznymi Stron.

ADMINISTRATOR **PODMIOT PRZETWARZAJĄCY**