

UMOWA NR ____/2026
POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w dniu ____ ____ 2026 r. we Wrocławiu pomiędzy:

Ekosystem sp. z o.o. z siedzibą we Wrocławiu (PNA: 54-203), przy ul. Legnickiej 51-53, wpisaną do Krajowego Rejestru Sądowego pod numerem 0000426169, NIP: 8992736747, REGON: 021916240, o kapitale zakładowym 14 311 000,00 zł,

zwaną dalej „**Powierzającym**”

którą reprezentuje:

.....

a

xxx z siedzibą w(e) xxx (PNA: xx-xxx), przy ul./al./pl. xxx, wpisaną do Krajowego Rejestru Sądowego pod numerem xxx, NIP: xxx, REGON: xxx, o kapitale zakładowym xxx zł,

zwaną/-ym dalej „**Przetwarzającym**”

którą reprezentuje ¹:

.....,

zwani/-e dalej łącznie „**Stronami**”, a każda z osobna „**Stroną**”,

o następującej treści:

§ 1. DEFINICJE

Użyte w niniejszej umowie określenia oznaczają:

- 1) **administrator** – administrator, w rozumieniu art. 4 pkt 7 RODO;
- 2) **dane osobowe** – dane osobowe, w rozumieniu art. 4 pkt 1 RODO;
- 3) **Dane Osobowe** – dane osobowe powierzone do przetwarzania w ramach Umowy;
- 4) **inspektor ochrony danych** – inspektor ochrony danych, w rozumieniu art. 37-39 RODO;
- 5) **podmiot przetwarzający** – podmiot przetwarzający, w rozumieniu art. 4 pkt 8 RODO;
- 6) **przetwarzanie** – przetwarzanie, w rozumieniu art. 4 pkt 2 RODO;
- 7) **RODO** – 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) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 oraz z 2018 r. Nr 127, str. 2);
- 8) **Umowa** – niniejsza umowa;

¹ nie dotyczy osób fizycznych / osób fizycznych prowadzących działalność gospodarczą;

- 9) **umowa źródłowa** – umowa lub inny dokument, z którego wynika świadczenie przez Przetwarzającego na rzecz Powierzającego usług związanych z przetwarzaniem, w rozumieniu art. 28 ust. 3 lit. g RODO, tj.²: umowa nr xxx z dnia xx.xx.2026 r.;
- 10) **ustawa o ochronie danych osobowych** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r., poz. 1781 z późn. zm.).

§ 2. WSTĘPNA WERYFIKACJA PRZETWARZAJĄCEGO (ART. 28 UST. 1 RODO)

Przed powierzeniem przetwarzania Danych Osobowych Przetwarzającemu, Powierzający dokonał wstępnej weryfikacji Przetwarzającego w oparciu o listę kontrolną – kryteria wyboru podmiotu przetwarzającego, któremu Powierzający zamierza powierzyć dane osobowe. Lista kontrolna, o której mowa w zdaniu poprzednim, po jej wypełnieniu i podpisaniu przez Przetwarzającego stanowić będzie załącznik nr 2 do Umowy.

§ 3. CEL, CHARAKTER I PRZEDMIOT PRZETWARZANIA DANYCH OSOBOWYCH (ART. 28 UST. 3 RODO)

1. Powierzający pełni rolę administratora Danych Osobowych.
2. Przetwarzający pełni rolę podmiotu przetwarzającego Dane Osobowe.
3. Dane Osobowe przetwarzane będą przez Przetwarzającego w celu realizacji umowy źródłowej.
4. Dane Osobowe będą przetwarzane w formie papierowej / w sposób zautomatyzowany, w systemach informatycznych / w formie papierowej i w sposób zautomatyzowany, w systemach informatycznych³.
5. W okresie obowiązywania umowy źródłowej Dane Osobowe przetworzone zostaną jednorazowo / kilkurazowo / Dane Osobowe przetwarzane będą stale, nie-jednorazowo, powtarzalnie⁴.
6. Zakres powierzonych do przetwarzania Przetwarzającemu Danych Osobowych wskazany został w załączniku nr 1 do Umowy, który zawiera w szczególności:
 - 1) datę sporządzenia załącznika, a w razie konieczności również inne oznaczenie (np. wersję załącznika), tak by w przypadku zmiany załącznika możliwym było jednoznaczne ustalenie jaki zakres Danych Osobowych mógł być przetwarzany w danym okresie przez Przetwarzającego,
 - 2) zakres powierzonych Przetwarzającemu do przetwarzania Danych Osobowych (w szczególności ich rodzaj)⁵,
 - 3) kategorie osób, których Dane Osobowe dotyczą⁶,

² należy wskazać nazwę i datę dokumentu, w którym Przetwarzający zobowiązał się wobec Powierzającego do świadczenia usług związanych z przetwarzaniem, w rozumieniu art. 28 ust. 3 lit. g RODO;

³ niepotrzebne skreślić;

⁴ niepotrzebne skreślić; jednorazowo (np. zostanie sporządzona lista obecności uczestników szkolenia), kilkurazowo (np. zostanie sporządzony kilka list obecności uczestników z kilku szkoleń odbywających się według ustalonego harmonogramu), stale, nie-jednorazowo, powtarzalnie (np. w przypadku umowy na serwis systemu komputerowego, gdzie podmiot przetwarzający ma dostęp do systemu i poprawia na bieżąco zgłaszane mu przez użytkowników błędy);

⁵ rodzaj danych: dane zwykłe lub dane wrażliwe (w rozumieniu motywu 10 preambuły RODO); należy wskazać jakie dane zwykłe (np. imię, nazwisko, adres zamieszkania, NIP, PESEL) oraz jakie dane wrażliwe (np. dane o zdrowiu, o orientacji seksualnej);

⁶ należy wskazać czyje dane są zbierane (np. klienci, wykonawcy, pacjenci, studenci, personel, osoby poszukujące pracy);

- 4) rodzaj operacji dokonywanych na Danych Osobowych⁷,
- 5) miejsce przetwarzania Danych Osobowych⁸, w szczególności dotyczy to przypadków przetwarzania Danych Osobowych w państwach trzecich lub przez organizacje międzynarodowe. Przetwarzający nie ma obowiązku wskazania w załączniku nr 1 do Umowy dokładnego adresu (ulica/plac/aleja/itp., nr domu, numer budynku) miejsca, w którym przetwarzane są Dane Osobowe, zobowiązuje się jednak do ich podania na żądanie Powierzającego (w szczególności w przypadku prowadzenia przez organ nadzorczy postępowania w sprawie naruszenia przepisów o ochronie danych osobowych w odniesieniu do Danych Osobowych) niezwłocznie, nie później jednak niż w terminie 48 godzin od zgłoszenia takiego żądania przez Powierzającego,
- 6) podpisy Stron.

§ 4. CZAS TRWANIA PRZETWARZANIA (ART. 28 UST. 3 RODO)

Umowa będzie obowiązywać, a Przetwarzający będzie przetwarzał Dane Osobowe przez okres świadczenia przez Przetwarzającego usług związanych z przetwarzaniem Danych Osobowych w ramach umowy źródłowej, z uwzględnieniem postanowień § 11.

§ 5. POLECENIE PRZETWARZANIA DANYCH (ART. 28 UST. 3 LIT. A RODO)

1. Powierzający poleca Przetwarzającemu oraz osobom działającym z upoważnienia Przetwarzającego przetwarzanie Danych Osobowych wyłącznie w zakresie wynikającym z RODO, ustawy o ochronie danych osobowych i Umowy oraz niezbędnym do świadczenia usług związanych z przetwarzaniem na podstawie umowy źródłowej.
2. Powierzający ~~nie wyraża zgody~~ / wyraża zgodę⁹ na przekazywanie Danych Osobowych do Państwa trzeciego lub organizacji międzynarodowej.
3. Przekazanie Danych Osobowych do państwa trzeciego lub organizacji międzynarodowej odbywa się w pełnej zgodności z obowiązującymi w tym zakresie przepisami, w szczególności rozdziałem V RODO. W zakresie w jakim przekazanie Danych Osobowych do państwa trzeciego lub organizacji międzynarodowej nie odbywa się na podstawie art. 45 RODO, Przetwarzający zobowiązany jest przed przekazaniem Danych Osobowych przedstawić Powierzającemu dokument potwierdzający, że kraj trzeci lub organizacja międzynarodowa – stosownie do art. 46 ust. 1 RODO – zapewniają odpowiednie zabezpieczenia i że obowiązują w nich egzekwowalne prawa osób, których dane dotyczą oraz skuteczne środki ochrony prawnej, tak by

⁷ operacje wykonywane na danych osobowych przez Przetwarzającego mogą obejmować: 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;

⁸ należy wskazać miejsce, gdzie dane osobowe będą przetwarzane, w tym obowiązkowo, gdzie dane będą przechowywane (np. w siedzibie Przetwarzającego; w oddziale Przetwarzającego w Elblągu, ul. Xyz 1/2, Elbląg; w serwerowni dostawcy poczty elektronicznej tj. XYZ sp. z o.o. z/s w Warszawie, ul. Xyz 1/2, Warszawa);

⁹ niepotrzebne skreślić;

Przetwarzający mógł wykazać spełnienie zasad wskazanych w art. 5 ust. 1 lit. a i ust. 2 RODO ¹⁰.

§ 6. OBOWIĄZEK ZACHOWANIA TAJEMNICY DANYCH OSOBOWYCH ORAZ SPOSOBÓW ICH ZABEZPIECZENIA (ART. 28 UST. 3 LIT. B RODO)

Przetwarzający zobowiązuje się do bezterminowego zachowania w tajemnicy Danych Osobowych oraz sposobów ich zabezpieczenia, w tym także po rozwiązaniu Umowy, oraz zobowiązuje się zapewnić, aby osoby upoważnione do przetwarzania Danych Osobowych ze strony Przetwarzającego zachowały bezterminowo Dane Osobowe oraz sposoby ich zabezpieczenia w tajemnicy, w tym także po rozwiązaniu Umowy, ustaniu zatrudnienia u Przetwarzającego lub zakończenia innego stosunku prawnego (praktyka, staż itp.), w ramach którego przetwarzały one Dane Osobowe na podstawie upoważnienia. W tym celu Przetwarzający dopuści do przetwarzania Danych Osobowych tylko osoby, które zostały upoważnione do przetwarzania tych danych oraz podpisały stosowne zobowiązanie do zachowania bezterminowo w tajemnicy Danych Osobowych oraz sposobów ich zabezpieczenia.

§ 7. BEZPIECZEŃSTWO PRZETWARZANIA (ART. 28 UST. 3 LIT. C RODO)

1. Przetwarzający oświadcza, że stosownie do przepisów art. 32 RODO wdrożył odpowiednie środki techniczne i organizacyjne zabezpieczające Dane Osobowe, oraz stale monitoruje adekwatność tych środków, w świetle wymagań stawianych w rzeczonym artykule RODO.
2. Przetwarzający obowiązany jest do prowadzenia i aktualizacji stosownej dokumentacji opisującej zastosowane środki, o których mowa w ust. 1.
3. Przetwarzający na każde żądanie Powierającego:
 - 1) udzieli mu wszelkich informacji dotyczących stosowanych przez Przetwarzającego środków technicznych i organizacyjnych zabezpieczających Dane Osobowe,
 - 2) umożliwi mu dokonanie przeglądu środków, o których mowa w pkt 1,
 - 3) udostępni mu dokumentację, o której mowa w ust. 2.

§ 8. DALSZE POWIERZENIE PRZETWARZANIA (PODPOWIERZENIE) (ART. 28 UST. 3 LIT. D / ART. 28 UST. 2 I 4 RODO)

1. Powierający ~~nie wyraża zgody~~ / wyraża zgodę ¹¹ na (dalsze) powierzenie (tzw. podpowierzenie) przetwarzania Danych Osobowych przez Przetwarzającego innym podmiotom, z uwzględnieniem treści § 5 ust. 2 i 3 ¹².
2. Przed podpowierzeniem przetwarzania Danych Osobowych, Przetwarzający jest zobowiązany poinformować pisemnie lub e-mail`owo Powierającego o zamiarze podpowierzenia przetwarzania Danych Osobowych.

¹⁰ ustęp 3 dotyczy tylko sytuacji, w której Powierający w ust. 2 wyraził zgodę na przekazanie Danych Osobowych do państwa trzeciego lub organizacji międzynarodowej;

¹¹ niepotrzebne skreślić;

¹² w przypadku niewyrażenia zgody na (dalsze) powierzenie przetwarzania Danych Osobowych, ust. 2-9 nie mają zastosowania;

3. Informacja o zamiarze podpowierzenia przetwarzania Danych Osobowych zawiera co najmniej:
 - 1) dane podmiotu, któremu Przetwarzający zamierza podpowierzyć przetwarzanie Danych Osobowych (imię i nazwisko / firmę oraz dane kontaktowe),
 - 2) informacje o:
 - a) charakterze i czasie trwania podpowierzenia,
 - b) celu ich przetwarzania przez podmiot, któremu będą podpowierane,
 - c) zakresie podpowierzanych Danych Osobowych (w szczególności ich rodzaju),
 - d) kategoriach osób, których Dane Osobowe miałyby być podpowierzone,
 - e) miejscu (adresie) przetwarzania Danych Osobowych przez podmiot, któremu będą podpowierane.
4. Jeżeli Powierający w terminie **14 dni** od otrzymania wszystkich powyższych informacji nie wyrazi sprzeciwu wobec zamiaru podpowierzenia przetwarzania Danych Osobowych wskazanemu podmiotowi, Przetwarzający może podpowierzyć przetwarzanie Danych Osobowych, zgodnie z tymi informacjami.
5. Podpowierzenie przetwarzania Danych Osobowych przez Przetwarzającego jest dopuszczalne tylko na podstawie umowy podpowierzenia.
6. Umowa podpowierzenia zostanie zawarta w formie pisemnej (przez którą rozumie się również formę elektroniczną) ¹³.
7. Na podstawie umowy podpowierzenia podmiot, któremu podpowierzono przetwarzanie Danych Osobowych zobowiąże się do spełniania takich samych obowiązków i wymogów, jak te które na mocy Umowy nałożone są na Przetwarzającego. W razie wątpliwości poczytuje się, że weryfikacja czy dalszy podmiot przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą odbywa się w – zgodny z RODO – sposób wybrany przez Przetwarzającego.
8. Jeżeli podmiot, któremu podpowierzono przetwarzanie Danych Osobowych nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Powierającego za wypełnienie obowiązków tego podmiotu spoczywa na Przetwarzającym.
9. Przetwarzający zobowiązany jest do niezwłocznego powiadomienia Powierającego, o każdym przypadku niewywiązywania się przez podmiot, któremu podpowierzono przetwarzanie Danych Osobowych, ze spoczywających na tym podmiocie obowiązków ochrony Danych Osobowych.

§ 9. WSPÓŁPRACA W ZAKRESIE ŻAŁAŃ OSOBY, KTÓREJ DANE DOTYCZĄ, WYNIKAJĄCYCH Z ROZDZIAŁU III RODO (ART. 28 UST. 3 LIT. E RODO)

1. Przetwarzający zobowiązuje się pomagać Powierającemu, poprzez odpowiednie środki techniczne i organizacyjne, w wywiązywaniu się z obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw określonych w art. 15-22 RODO.

¹³ zob. art. 28 ust. 9 RODO

2. W przypadku, gdy osoba, której dane dotyczą skieruje żądanie realizacji jej praw, o których mowa w art. 15-22 RODO, bezpośrednio do Przetwarzającego, Przetwarzający zobowiązany jest przekazać niezwłocznie treść tego żądania (w szczególności treść sprzeciwu, o którym mowa w art. 21 RODO) do Powierzającego. Ponadto, jeżeli Powierzający nie będzie mógł zrealizować żądań osoby, której dane dotyczą, bez współdziałania Przetwarzającego, Przetwarzający na polecenie Powierzającego podejmie wskazane przez Powierzającego czynności, a w szczególności:
- 1) w razie zgłoszenia przez osobę, której dane dotyczą żądania prawa dostępu, o którym mowa w art. 15 RODO – przygotuje raport dla Powierzającego, zawierający informacje o przetwarzanych przez Przetwarzającego danych osobowych osoby zgłaszającej żądanie realizacji praw z art. 15 RODO i przekaze ten raport Powierzającemu;
 - 2) w razie zgłoszenia przez osobę, której dane dotyczą prawa do sprostowania danych, o którym mowa w art. 16 RODO – sprostuje dane osobowe osoby zgłaszającej żądanie realizacji praw z art. 16 RODO, poprzez nadpisanie danych osobowych tej osoby w systemach Przetwarzającego;
 - 3) w razie zgłoszenia przez osobę, której dane dotyczą prawa do bycia zapomnianym, o którym mowa w art. 17 RODO – usunie dane osobowe, osoby zgłaszającej żądanie realizacji praw z art. 17 RODO, ze wszystkich systemów Przetwarzającego, w których mogą się znaleźć dane osobowe tej osoby, w szczególności z systemów źródłowych agregujących dane. W terminie do 7 dni od zgłoszenia przez Powierzającego polecenia usunięcia danych Przetwarzający potwierdzi usunięcie danych Powierzającemu;
 - 4) w razie zgłoszenia przez osobę, której dane dotyczą prawa do ograniczenia przetwarzania, o którym mowa w art. 18 RODO – nie później niż w ciągu 24 godzin od przedstawienia takiego polecenia przez Powierzającego, czasowo zablokuje możliwości edycji rekordów (poprzez stosowną funkcjonalność systemu informatycznego lub inne działanie, w tym organizacyjne, które skutecznie zapewni, że nie dojdzie do zmiany rekordów) dotyczących, osoby zgłaszającej żądanie realizacji praw z art. 18 RODO;
 - 5) w razie zgłoszenia przez osobę, której dane dotyczą prawa do przenoszenia danych, o którym mowa w art. 20 RODO – wyeksportuje do Powierzającego wszystkie przetwarzane elektronicznie dane osobowe dotyczące osoby zgłaszającej żądanie realizacji praw z art. 20 RODO.

§ 10. POMOC W REALIZACJI OBOWIĄZKÓW OKREŚLONYCH W ART. 32-36 RODO (ART. 28 UST. 3 LIT. F RODO)

1. Przetwarzający zobowiązuje się pomagać Powierzającemu w wywiązywaniu się z obowiązków określonych w art. 32-36 RODO.
2. W ramach realizacji obowiązków, o których w ust. 1, Przetwarzający ma w szczególności obowiązek:
 - 1) wyznaczenia osób odpowiedzialnych za podjęcie: kroków w celu zaradzenia naruszeniu ochrony Danych Osobowych i - w uzgodnieniu z Powierzającym - stosownych działań naprawczych;

- 2) jeżeli Przetwarzający stwierdzi, że przetwarzane przez niego dane osobowe są nieprawidłowe lub nieaktualne - niezwłocznego zawiadomienia o tym fakcie Powierzającego;
- 3) zawiadamiania Powierzającego o wszelkich naruszeniach ochrony Danych Osobowych. Zawiadomienie powinno nastąpić niezwłocznie, nie później jednak niż w ciągu **24 godzin** od stwierdzenia przez Przetwarzającego naruszenia ochrony Danych Osobowych. Zawiadomienie powinno zawierać informacje, które pozwolą Powierzającemu na przygotowanie zawiadomienia zgodnie z art. 33 ust. 3 RODO (w zakresie art. 33 ust. 3 lit. b RODO Przetwarzający powinien wskazać dane inspektora ochrony danych Przetwarzającego lub oznaczenie innego punktu kontaktowego Przetwarzającego, od którego można uzyskać więcej informacji);
- 4) dokumentowania naruszeń ochrony Danych Osobowych, zgodnie z art. 33 ust. 5 RODO – tj. dokumentowania m.in. okoliczności naruszenia ochrony danych osobowych, jego skutków oraz podjętych działań zaradczych, w sposób umożliwiający organowi nadzorczemu zweryfikowanie na podstawie tej dokumentacji przestrzegania przez Powierzającego i Przetwarzającego art. 33 RODO;
- 5) udzielania Powierzającemu informacji potrzebnych do dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, o której mowa w art. 35 RODO;
- 6) udzielania Powierzającemu informacji potrzebnych do konsultacji z organem nadzorczym w zakresie oceny skutków dla ochrony danych, o których mowa w art. 36 RODO.

§ 11. ZAKOŃCZENIE POWIERZENIA PRZETWARZANIA (ART. 28 UST. 3 LIT. G RODO)

1. Niezwłocznie po zakończeniu świadczenia przez Przetwarzającego usług związanych z przetwarzaniem Danych Osobowych, jednakże nie później niż w terminie **14 dni** od zakończenia świadczenia tych usług, Przetwarzający zależnie od decyzji Powierzającego:
 - 1) usuwa Dane Osobowe albo
 - 2) zwraca Powierzającemu wszelkie Dane Osobowe oraz usuwa wszelkie ich istniejące kopie.
2. Przetwarzający potwierdzi usunięcie lub zwrot Danych Osobowych oraz ich kopii pisemnym protokołem podpisanym przez osobę uprawnioną do składania oświadczeń woli w imieniu Przetwarzającego i umożliwi – na żądanie Powierzającego – przeprowadzenie przez Powierzającego audytu zgodnie z § 12.
3. Stosownie do treści art. 28 ust. 3 lit. g RODO po zakończeniu świadczenia usług związanych z przetwarzaniem Przetwarzający może przetwarzać Dane Osobowe, w zakresie w jakim prawo Unii lub prawo państwa członkowskiego nakazuje przechowywanie Danych Osobowych.

**§ 12. UDOSTĘPNIANIE INFORMACJI O POWIERZENIU I WERYFIKACJA
PRZESTRZEGANIA ZASAD PRZETWARZANIA DANYCH OSOBOWYCH
(ART. 28 UST. 3 LIT. H RODO)**

1. Przetwarzający zobowiązuje się udostępnić Powierzającemu wszelkie informacje niezbędne do wykazania przez Powierzającego oraz Przetwarzającego spełnienia obowiązków, o których mowa w art. 28 RODO.
2. Powierzający jest uprawniony do weryfikacji przestrzegania przez Przetwarzającego zasad przetwarzania Danych Osobowych wynikających z RODO, ustawy o ochronie danych osobowych oraz Umowy, w szczególności poprzez:
 - 1) prawo żądania udzielenia wszelkich informacji dotyczących powierzonych Danych Osobowych, w tym informacji o dokładnych lokalizacjach, w których Przetwarzający lub jego (pod)przetwarzający przetwarzają Dane Osobowe,
 - 2) prawo przeprowadzania audytów lub inspekcji Przetwarzającego w zakresie zgodności operacji przetwarzania z prawem i z Umową ¹⁴.
3. Powierzający ma obowiązek poinformowania Przetwarzającego o planowanym audycie na **7 dni** przed jego rozpoczęciem. Audyt nie może trwać dłużej niż miesiąc od jego rozpoczęcia.
4. Audyt lub inspekcja przeprowadzane są przez **upoważnionych audytorów**, przez których w ramach niniejszego paragrafu rozumie się, upoważnionego przez Powierzającego:
 - 1) pracownika Powierzającego lub
 - 2) audytora zewnętrznego.
5. Upoważniony audytor ma prawo w szczególności do:
 - 1) wstępu i oględzin (zwłaszcza sposobu zabezpieczenia) pomieszczeń, w których przetwarzane są Dane Osobowe,
 - 2) przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania Danych Osobowych,
 - 3) wglądu do wszelkich dokumentów i wszelkich informacji mających bezpośredni związek z powierzeniem przetwarzania Danych Osobowych na podstawie Umowy,
 - 4) żądania złożenia ustnych lub pisemnych wyjaśnień przez Przetwarzającego oraz personel Przetwarzającego (w szczególności pracowników), w zakresie niezbędnym do ustalenia stanu faktycznego.
6. Po zakończeniu audytu upoważniony audytor przedstawia wynik audytu w postaci raportu.
7. W przypadku naruszenia ochrony Danych Osobowych u Przetwarzającego lub rażącego naruszenia przez Przetwarzającego przepisów o ochronie danych osobowych, Powierzający ma prawo do przeprowadzenia u Przetwarzającego niezapowiedzianej darmowej inspekcji.
8. Powierzający może w szczególności przeprowadzić:

¹⁴ sposób audytu będzie uwzględniać specyfikę powierzenia przetwarzania;

- 1) darmowy audyt, na odległość, z wykorzystaniem listy weryfikacyjnej – w przeciągu 3 (trzech) pierwszych miesięcy od powierzenia przetwarzania Danych Osobowych Przetwarzającemu,
 - 2) darmowy audyt, w dowolny sposób – 1 (jeden) raz, w każdym roku obowiązywania Umowy,
 - 3) darmowy audyt lub inspekcję, w dowolny sposób – po każdym naruszeniu, o którym mowa w ust. 7,
 - 4) darmowy audyt, o który mowa w § 11 ust. 2, w dowolny sposób – po zakończeniu Umowy.
9. W razie wątpliwości poczytuje się, że:
- 1) okoliczności umożliwiające przeprowadzenie audytu lub inspekcji, o których mowa w ust. 8 pkt 1-4 nie wykluczają się wzajemnie ¹⁵;
 - 2) darmowa inspekcja / darmowy audyt oznacza, że za podejmowane w ramach inspekcji lub audytu czynności Przetwarzający nie nabywa względem Powierzającego jakichkolwiek wierzytelności (np. o zwrot kosztów czy wynagrodzenie dla pracowników Przetwarzającego biorących udział w inspekcji lub audycie).
10. Jeżeli zdaniem Przetwarzającego wydane mu przez Powierzającego polecenie stanowi naruszenie przepisów RODO lub innych powszechnie obowiązujących przepisów o ochronie danych osobowych Przetwarzający zobowiązuje się niezwłocznie poinformować o tym fakcie Powierzającego.

§ 13. REJESTR WSZYSTKICH KATEGORII CZYNNOŚCI PRZETWARZANIA (ART. 30 UST. 2 I 3 RODO)

Przetwarzający oświadcza, że w związku z zawarciem Umowy, będzie prowadził rejestr wszystkich kategorii czynności przetwarzania, w rozumieniu art. 30 ust. 2 i 3 RODO, dokonywanych w imieniu Powierzającego. Rejestr ten, w zakresie dotyczącym Powierzającego, Przetwarzający udostępni Powierzającemu, na każde żądanie Powierzającego.

§ 14. WYZNACZENIE INSPEKTORA OCHRONY DANYCH (ART. 37 RODO)

1. Powierzający wyznaczył inspektora ochrony danych:
imię i nazwisko: Zuzanna Łukaszewska
służbowy adres poczty elektronicznej: iodo@ekosystem.wroc.pl
służbowy nr telefonu: +48 797 195 951
2. Przetwarzający wyznaczył inspektora ochrony danych / osobę kontaktową w sprawach dotyczących Danych Osobowych ¹⁶:
imię i nazwisko: _____
służbowy nr telefonu: _____

¹⁵ przykład: jeżeli Umowa będzie obowiązywała przez 6 miesięcy danego roku i w trakcie jej obowiązywania zaistniało 1 (jedno) naruszenie ochrony danych: możliwe jest przeprowadzenie czterech audytów po jednym na każdą okoliczność wymienioną w ust. 8 pkt 1-4;

¹⁶ niepotrzebne skreślić;

służbowy adres poczty elektronicznej: _____

3. W przypadku zmiany osób, o których mowa w ust. 1 lub 2, Strona u której doszło do zmiany danych tej osoby, zobowiązana jest do niezwłocznego zawiadomienia o tym drugiej Strony, na adres e-mail wskazany w ust. 1 lub 2 (w zależności od tego czy o zmianie zawiadamia Przetwarzający czy Powierający) wraz ze wskazaniem aktualnych danych, o których mowa odpowiednio w ust. 1 lub 2.

§ 15. POSTANOWIENIA DODATKOWE (ART. 28 UST. 3 RODO)

1. Przetwarzający odpowiada na zasadach ogólnych za szkody, jakie powstaną u Powierającego lub osób trzecich w wyniku naruszenia przez Przetwarzającego przepisów prawa lub niewykonania lub nienależytego wykonania Umowy przez Przetwarzającego.
2. Każda ze Stron zobowiązana jest do poinformowania osób przez siebie upoważnionych do określonych czynności w związku z realizacją Umowy lub umowy źródłowej (w szczególności osób reprezentujących stronę lub osób kontaktowych), o tym, że druga Strona będzie przetwarzała ich dane osobowe jako administrator, w celach, niezbędnych do należytego wykonania Umowy i umowy źródłowej oraz do wypełnienia wynikających z powszechnie obowiązujących przepisów obowiązków prawnych ciążących na Stronach jako administratorach danych. Poinformowanie, o którym mowa w zdaniu poprzednim, będzie zawierać ponadto taką treść, która umożliwi drugiej stronie ewentualne powołanie się na art. 14 ust. 5 lit. a RODO.
3. W celu realizacji obowiązku, o którym mowa w ustępie poprzedzającym zd. 2, Powierający w załączniku nr 3 do Umowy przekazuje Przetwarzającemu treść obowiązku informacyjnego dla personelu Przetwarzającego. Przetwarzający zobowiązany jest w terminie 7 dni od zawarcia Umowy do przekazania Powierającemu treści obowiązku informacyjnego, o którym mowa w art. 14 RODO, dla personelu Powierającego, a po tym terminie, zobowiązany będzie względem tego personelu do samodzielnej realizacji obowiązku informacyjnego, o którym mowa w art. 14 RODO.

§ 16. POSTANOWIENIA KOŃCOWE

1. O ile co innego nie wynika wyraźnie z Umowy (np. § 14 ust. 3), wszelkie zmiany Umowy wymagają formy pisemnej (przez którą rozumie się również formę elektroniczną, w rozumieniu kodeksu cywilnego) pod rygorem nieważności.
2. Spory związane z wykonywaniem Umowy rozstrzygane będą przez sąd właściwy miejscowo i rzeczowo dla siedziby Powierającego (tj. ul. Legnicka 51-53, 54-203 Wrocław).
3. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

§ 17. ZAŁĄCZNIKI

Integralną część Umowy stanowią następujące załączniki:

- 1) szczegóły powierzenia przetwarzania danych,
- 2) lista kontrolna - kryteria wyboru podmiotu przetwarzającego, któremu administrator zamierza powierzyć dane osobowe,

- 3) wzór klauzuli informacyjnej stosowanej przez Powierzającego, do wykonania obowiązku z art. 14 RODO względem osób realizujących umowę.

Powierzający

Przetwarzający

Wrocław, dnia ____ ____ 2026 r.

SZCZEGÓŁY POWIERZENIA
(ADMINISTRATORZY, ZBIORY / RODZAJE I ZAKRES DANYCH, KATEGORIE OSÓB, RODZAJ OPERACJI PRZETWARZANIA,
LOKALIZACJE PRZETWARZANIA)

| L.P. | Nazwa i dane kontaktowe administratora Danych Osobowych | Nazwa zbioru/czynności przetwarzania oraz rodzaj i zakres powierzanych Danych Osobowych ¹ | Kategorie osób, których Dane Osobowe dotyczą | Rodzaj operacji przetwarzania ² | Lokalizacje Przetwarzającego, w których przetwarzane będą dane osobowe |
|------|---|--|---|---|--|
| 1 | Ekosystem sp. z o.o. ul. Legnicka 51-53, 54-203 Wrocław ekosystem@ekosystem.wroc.pl 71 75 86 911 | Zbiór: Dane pracowników i współpracowników Rodzaj: dane zwykłe Zakres: imię i nazwisko, służbowy adres e-mail, numer telefonu, nazwa stanowiska, miejsce w strukturze organizacyjnej, zakres obowiązków i odpowiedzialności, poziomy dostępu do systemów informatycznych, historia szkoleń z zakresu bezpieczeństwa (podczas audytu zgodności). | pracownicy, współpracownicy | dostęp, przeglądanie, analiza, weryfikacja, audytowanie | |
| 2 | j.w. | Zbiór: Dane techniczne i logi systemowe Rodzaj: dane zwykłe Zakres: loginy użytkowników, adresy IP przypisane do użytkowników, logi systemowe, listy kontroli dostępu (ACL) | pracownicy, współpracownicy, użytkownicy systemów | j.w. | |

¹ jeżeli Dane Osobowe nie są przetwarzane w nazwanym zbiorze, należy wskazać wyłącznie rodzaj (tj. dane zwykłe oraz – jeżeli są przetwarzane – dane wrażliwe) oraz zakres danych np. dane zwykłe: imię i nazwisko, adres zamieszkania, telefon; dane wrażliwe: dane o zdrowiu;

² **operacje wykonywane na danych osobowych przez Przetwarzającego mogą obejmować:** 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

| L.P. | Nazwa i dane kontaktowe administratora Danych Osobowych | Nazwa zbioru/czynności przetwarzania oraz rodzaj i zakres powierzanych Danych Osobowych ¹ | Kategorie osób, których Dane Osobowe dotyczą | Rodzaj operacji przetwarzania ² | Lokalizacje Przetwarzającego, w których przetwarzane będą dane osobowe |
|------|---|---|---|--|--|
| 3 | j.w. | Zbiór: Dane klientów i kontrahentów Rodzaj: dane zwykłe Zakres: dane osobowe przetwarzane w systemach i dokumentacji administratora, do których dostęp jest niezbędny podczas audytów, analiz bezpieczeństwa, testów i innych usług objętych umową | klienci, przedstawiciele klientów, kontrahenci, przedstawiciele kontrahentów | dostęp, przeglądanie, analiza, testowanie, audytowanie | |

Powierzający

Przetwarzający

**LISTA KONTROLNA - KRYTERIA WYBORU PODMIOTU PRZETWARZAJĄCEGO,
KTÓREMU POWIERZAJĄCY ZAMIERZA POWIERZYĆ PRZETWARZANIE DANYCH OSOBOWYCH**

Niniejsze kryteria stworzone zostały w celu wstępnej weryfikacji podmiotu przetwarzającego, w zakresie spełniania przez niego podstawowych wymogów RODO.

Kryteria wyboru podmiotu przetwarzającego oparte zostały o:

- 1) art. 28 ust. 1 RODO, zgodnie z którym *„1. Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą”* oraz
- 2) motyw 81 RODO, zgodnie z którym: *„(81) Aby zapewnić przestrzeganie wymogów niniejszego rozporządzenia w przypadku przetwarzania, którego w imieniu administratora ma dokonać podmiot przetwarzający, administrator powinien, powierzając podmiotowi przetwarzającemu czynności przetwarzania, korzystać z usług wyłącznie podmiotów przetwarzających, które zapewniają wystarczające gwarancje – w szczególności jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby – wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom niniejszego rozporządzenia, w tym wymogom bezpieczeństwa przetwarzania. Stosowanie przez podmiot przetwarzający zatwierdzonego kodeksu postępowania lub zatwierdzonego mechanizmu certyfikacji może posłużyć za element wykazujący wywiązywanie się z obowiązków administratora”*.

ADMINISTRATOR Ekosystem sp. z o.o. z siedzibą we Wrocławiu, numer KRS: 0000426169
(dalej również **Administrator**)

PODMIOT PRZETWARZAJĄCY
(dalej również **PP**): _____
(nazwa podmiotu, adres siedziby, KRS/NIP – jeżeli zostały nadane)

DOTYCZY UMOWY / ZAMÓWIENIA:
(dalej **umowa źródłowa**) _____

PLANOWANY OKRES POWIERZENIA PRZETWARZANIA: _____

| L.p. | PYTANIE | ODPOWIEDŹ |
|-------------------------------------|---|-----------|
| SEKCJA I: PYTANIA PODSTAWOWE | | |
| 1. | <p>Czy PP będzie wykorzystywać / przetwarzać dane osobowe powierzone przez Administratora (dalej Dane Osobowe) we własnych celach / na własne potrzeby lub w celach / na potrzeby podmiotów innych niż Administrator?</p> <p><i>(Jeżeli odpowiedź jest twierdząca, proszę wskazać również: 1) jaki zakres Danych Osobowych PP zamierza wykorzystywać/przetwarzać, w tym w szczególności czy zamierza przetwarzać dane telemetryczne; 2) w jakim i czym celu / na jakie i czyje potrzeby będzie przetwarzał Dane Osobowe, w szczególności czy PP zamierza przetwarzać te dane w celu ulepszania własnych produktów/usług lub celach marketingowych)</i></p> | |
| 2. | <p>Czy realizując umowę źródłową PP korzystał będzie z usług podmiotów zewnętrznych / podwykonawców, którym udostępni / powierzy Dane Osobowe (uwaga: za takie podmioty uważa się np. podmioty świadczące usługę poczty e-mail na rzecz PP)?</p> | |
| 3. | <p>Czy w celu świadczenia przez PP usług związanych z przetwarzaniem, w rozumieniu art. 28 ust. 3 lit. h RODO, Dane Osobowe będą przekazywane do państwa trzeciego lub organizacji międzynarodowej, w rozumieniu rozdziału V RODO?</p> | |

| L.p. | PYTANIE | ODPOWIEDŹ |
|----------------------------------|--|-----------|
| | <i>(Jeżeli odpowiedź jest twierdząca, proszę wskazać również: 1) nazwy i siedziby podmiotów (w tym PP, jeżeli PP zamierza przetwarzać Dane Osobowe w państwie trzecim) oraz 2) w których państwach podmioty te miałyby przetwarzać Dane Osobowe lub przez które organizacje międzynarodowe Dane Osobowe miałyby być przetwarzane.)</i> | |
| 4. | <p>Czy PP posiada referencje od innych podmiotów, które obsługuje / obsługiwał i u których w ramach świadczonej obsługi przetwarzał dane osobowe jako podmiot przetwarzający?</p> <p><i>(Jeżeli odpowiedź jest twierdząca proszę wskazać również podmioty od których PP posiada takie referencje.)</i></p> | |
| SEKCJA II: WIEDZA FACHOWA | | |
| 5. | <p>Czy PP wyznaczył inspektora ochrony danych w rozumieniu art. 37-39 RODO?</p> <p><i>(Jeżeli odpowiedź jest twierdząca, proszę wskazać również aktualne informacji kontaktowe do inspektora ochrony danych PP, w szczególności proszę wskazać dane dla wszystkich przewidzianych przez PP form kontaktu z inspektorem np. adres korespondencyjny, adres e-mail, numer faksu, numer telefonu.)</i></p> | |
| 6. | Czy PP wyznaczył inną niż inspektor ochrony danych osobę / zespół odpowiedzialny za nadzór nad ochroną danych osobowych u PP? | |

| L.p. | PYTANIE | ODPOWIEDŹ |
|---------------------------|---|-----------|
| | <p><i>(Jeżeli odpowiedź jest twierdząca, proszę wskazać również aktualne informacje kontaktowe do tych osób, w szczególności proszę wskazać dane dla wszystkich przewidzianych przez PP form kontaktu z tymi osobami np. adres korespondencyjny, adres e-mail, numer faksu, numer telefonu.)</i></p> | |
| 7. | <p>Czy wszystkie osoby po stronie PP dedykowane do obsługi Powierzającego w ramach realizacji umowy źródłowej zostały przeszkolone i zapoznane z przepisami o ochronie danych osobowych?</p> <p><i>(Jeżeli odpowiedź jest twierdząca, proszę wskazać również przykłady dokumentów stosowanych przez PP, które potwierdzają powyższe okoliczności np. świadectwo ze szkolenia, certyfikat ze szkolenia, oświadczenie pracownika o odbyciu szkolenia.)</i></p> | |
| SEKCJA III: ZASOBY | | |
| 8. | <p>Czy PP wdrożył procedurę/instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych?</p> <p><i>(Jeżeli odpowiedź jest twierdząca, proszę wskazać przykłady dokumentów stosowanych przez PP, które potwierdzają powyższej okoliczności, np. polityka bezpieczeństwa informacji, polityka ochrony danych osobowych, zbiór najlepszych praktyk dla ochrony danych osobowych, procedura / instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych.)</i></p> | |

| L.p. | PYTANIE | ODPOWIEDŹ |
|------|--|-----------|
| 9. | Czy PP (jako administrator) dokumentuje wszelkie naruszenia ochrony danych osobowych, zgodnie z art. 33 ust 5 RODO? | |
| 10. | Czy PP prowadzi rejestry czynności przetwarzania danych osobowych (jako administrator oraz jako procesor), o których mowa w art. 30 RODO? | |
| 11. | <p>Czy PP wdrożył zasady, standardy, regulaminy, procedury, polityki, biblioteki, zbiory najlepszych praktyk lub inne dokumenty mające znaczenie dla ochrony danych osobowych (np. polityka bezpieczeństwa informacji, polityka ochrony danych osobowych, zbiór najlepszych praktyk dla ochrony danych osobowych)?</p> <p><u>(Jeżeli odpowiedź jest twierdząca proszę wskazać również przykłady dokumentów stosowanych przez PP, w których ujęto ww. zasady, standardy, regulaminy.)</u></p> | |
| 12. | Czy PP podda się audytowi przetwarzania Danych Osobowych przeprowadzonemu / inspekcji przetwarzania Danych Osobowych przeprowadzanej przez Administratora lub audytora upoważnionego przez Administratora? | |
| 13. | Czy wszystkie osoby delegowane przez PP do obsługi Administratora posiadają nadane upoważnienia do przetwarzania Danych Osobowych? | |

| L.p. | PYTANIE | ODPOWIEDŹ |
|--|--|-----------|
| | <i>(Jeżeli odpowiedź jest twierdząca, proszę wskazać również przykłady dokumentów stosowanych przez PP potwierdzających powyższe okoliczności, np. samodzielne pisemne oświadczenie PP o upoważnieniu pracownika do przetwarzania danych; upoważnienie do przetwarzania zawarte w umowie o pracę.)</i> | |
| 14. | <p>Czy wszystkie osoby upoważnione przez PP do przetwarzania Danych Osobowych zostały obowiązane do zachowania tych danych, jak i sposobów ich zabezpieczenia, w tajemnicy?</p> <p><i>(Jeżeli odpowiedź jest twierdząca, proszę wskazać również przykłady dokumentów stosowanych przez PP potwierdzających powyższe okoliczności, np. pisemne oświadczenie pracownika o zachowaniu poufności, zawarte w umowie o pracę.)</i></p> | |
| 15. | Czy obowiązek, o którym mowa w poprzedniej pozycji listy, rozciąga się również na okres po ustaniu zatrudnienia lub zakończenia innego stosunku prawnego (praktyka, staż, itp.) w związku z którym dana osoba była upoważniona do przetwarzania Danych Osobowych? | |
| SEKCJA IV: RETENCJA I USUWANIE DANYCH | | |
| 16. | Przez jaki okres PP przetwarzał będzie Dane Osobowe? | |
| 17. | Czy Dane Osobowe, dla których nie istnieją dla PP podstawy do przetwarzania są trwale usuwane? | |

| L.p. | PYTANIE | ODPOWIEDŹ |
|---------------------------------|---|-----------|
| | <p><i>(Jeżeli odpowiedź jest twierdząca, proszę wskazać w jaki sposób usuwane są dane np. dane w formie papierowej niszczone są w niszczarkach; dane w formie elektronicznej usuwane są z systemu za pomocą specjalistycznego oprogramowania do usuwania danych uniemożliwiającego ich odtworzenie. Jeżeli dane niszczone są w niszczarkach proszę o wskazanie poziomu bezpieczeństwa niszczarki P-1, P-2, etc.)</i></p> | |
| SEKCJA V: BEZPIECZEŃSTWO | | |
| 18. | Czy PP wdrożył następujące zasady zarządzania bezpieczeństwem informacji: | |
| a) | <p>system zarządzania bezpieczeństwem informacji na podstawie normy ISO 27001?</p> <p><i>(Jeżeli odpowiedź jest twierdząca, proszę wskazać również, którą wersję (rok) normy wdrożył).</i></p> | |
| b) | <p>zasady zarządzania bezpieczeństwem informacji z elementami wykorzystania normy ISO 27002?</p> <p><i>(Jeżeli odpowiedź jest twierdząca, proszę wskazać również, którą wersję (rok) normy wdrożył).</i></p> | |
| c) | <p>zasady zarządzania bezpieczeństwem informacji zgodne z wymaganiami Krajowych Ram Interoperacyjności?</p> | |
| 19. | Czy PP wdrożył inne, niż wskazane w poprzedniej pozycji listy, zasady ochrony informacji, tj: | |

| L.p. | PYTANIE | ODPOWIEDŹ |
|------|---|-----------|
| a) | <p>czy PP wdrożył: Ramy prywatności – PN-ISO/IEC 29100, Praktyczne zasady ochrony informacji o identyfikowalnych osobach – PN-ISO/IEC 29151, wytyczne dotyczące oceny skutków dla prywatności – PN-ISO/IEC 29131?</p> <p><u>(Jeżeli odpowiedź jest twierdząca, proszę również wskazać nazwy norm, które wdrożył).</u></p> | |
| b) | <p>czy PP wdrożył inne niż wymienione w lit. a zasady, standardy, regulaminy, procedury, polityki, biblioteki lub zbiory najlepszych praktyk mające znaczenie dla ochrony danych osobowych (np. polityka bezpieczeństwa informacji, polityka ochrony danych osobowych, zbiór najlepszych praktyk dla ochrony danych osobowych)?</p> <p><u>(Jeżeli odpowiedź jest twierdząca, proszę wskazać również nazwy ww. zasad, standardów, regulaminów, itd.)</u></p> | |
| 20. | <p>Czy PP ma procedurę opisującą w jaki sposób chronione są/będą Dane Osobowe w formie papierowej i elektronicznej?</p> <p><u>(Jeżeli odpowiedź jest twierdząca, proszę wskazać również przykłady dokumentów stosowanych przez PP, które potwierdzają powyższe okoliczności np. polityka ochrony danych; wykaz zabezpieczeń danych osobowych).</u></p> | |

| L.p. | PYTANIE | ODPOWIEDŹ |
|------|---|-----------|
| 21. | <p>Czy pracownicy zostali zapoznani z funkcjonującymi u PP procedurami i środkami bezpieczeństwa przetwarzania Danych Osobowych?</p> <p><i>(Jeżeli odpowiedź jest twierdząca, proszę wskazać również przykłady dokumentów stosowanych przez PP, które potwierdzają powyższe okoliczności np. świadectwo ze szkolenia, certyfikat ze szkolenia, oświadczenie pracownika o odbyciu szkolenia).</i></p> | |
| 22. | <p>Czy PP dba o bieżące doskonalenie wiedzy swoich pracowników poprzez cykliczne szkolenia oraz inne działania mające na celu uświadamianie pracowników w zakresie zagadnień dotyczących ochrony danych osobowych?</p> <p><i>(Jeżeli odpowiedź jest twierdząca, proszę wskazać również jakie działania podejmowane są przez PP w celu doskonalenia wiedzy pracowników oraz częstotliwość tych działań).</i></p> | |
| 23. | <p>Czy pracownicy PP pozwalają/ pozwolą na przebywanie w obszarze przetwarzania Danych Osobowych osób nieuprawnionych bez nadzoru?</p> | |
| 24. | <p>Czy PP przeprowadzał jakiegokolwiek szacowanie ryzyka pod kątem ochrony danych osobowych (w szczególności ocenę skutków planowanych operacji przetwarzania dla ochrony danych osobowych, o którym mowa w art. 35 ust. 1 RODO)?</p> | |

| L.p. | PYTANIE | ODPOWIEDŹ |
|------|---|-----------|
| | <i>(Jeżeli odpowiedź jest twierdząca, proszę wskazać również w jakim celu to szacowanie było prowadzone przez PP / do czego to szacowanie było PP potrzebne.)</i> | |
| 25. | <p>Czy PP okresowo przeprowadza kolejne działania związane z szacowaniem ryzyka pod kątem ochrony danych osobowych?</p> <p><i>(Jeżeli odpowiedź jest twierdząca, proszę wskazać również częstotliwości prowadzenia takich działań.)</i></p> | |
| 26. | <p>Czy PP prowadzi regularnie audyty dotyczące zasad bezpieczeństwa danych osobowych, w celu weryfikacji spełniania wymogów polityki ochrony danych lub innej wewnętrznej procedury, w tym oceny skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania?</p> <p><i>(Jeżeli odpowiedź jest twierdząca, proszę wskazać również częstotliwości prowadzenia takich audytów oraz czy są to audyty wewnętrzne (prowadzone przez pracowników PP), czy zewnętrzne (prowadzone przez firmy zewnętrzne).)</i></p> | |
| 27. | <p>Czy wnioski z audytów, o których mowa w poprzedniej pozycji tabeli, zostały udokumentowane?</p> | |

| L.p. | PYTANIE | ODPOWIEDŹ |
|------|--|-----------|
| | <i>(Jeżeli odpowiedź jest twierdząca, proszę wskazać również w postaci jakiego dokumentu zostały udokumentowane.)</i> | |
| 28. | Czy PP wdrożył odpowiednie środki techniczne i organizacyjne, które zapewniają procesowi przetwarzania danych osobowych stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze | |
| | w tym: | |
| a) | pseudonimizację i szyfrowanie Danych Osobowych, | |
| b) | zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, | |
| c) | zdolność do szybkiego przywrócenia dostępności Danych Osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego, <i>(Proszę wskazać również czy i jak często PP będzie robił kopie zapasowe wszystkich Danych Osobowych).</i> | |
| d) | regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania. <i>(Jeżeli PP będzie robił kopie zapasowe wszystkich Danych Osobowych proszę wskazać również czy i jak często PP będzie testował kopie zapasowe</i> | |

| L.p. | PYTANIE | ODPOWIEDŹ |
|------|---|-----------|
| | <u>Danych Osobowych, pod kątem możliwości prawidłowego i pełnego odtworzenia z nich tych danych.)</u> | |
| 29. | Czy pracownicy PP będą przechowywać, korzystać i transportować dokumenty zawierające Dane Osobowe w sposób uniemożliwiający zapoznanie się z ich treścią przez osoby nieupoważnione do przetwarzania Danych Osobowych? | |
| 30. | W kontekście pytania w poprzedniej pozycji listy – czy Dane Osobowe przetwarzane w formie papierowej, w sytuacji, gdy nie ma konieczności ich wykorzystania w bieżącej pracy (w tym po zakończeniu pracy), przechowywane są/będą zamykanych na zamek szafach / szafkach / szufladach, do których nie mają dostępu osoby nieupoważnione? | |
| 31. | Czy, po godzinach pracy organizacji PP, osoby inne niż uprawnione do przetwarzania danych (np. firma sprzątająca, ochrona), mają za zgodą lub wiedzą PP dostęp do pomieszczeń, w których ma miejsce przetwarzanie danych osobowych? <u>(Jeżeli odpowiedź jest twierdząca, proszę wskazać również jakie podmioty mogą mieć za wiedzą lub zgodą PP dostęp do pomieszczeń, w których przetwarzane są Dane Osobowe.)</u> | |
| 32. | Czy osoby, o których mowa w poprzedniej pozycji listy, zostały zobowiązane do zachowania danych osobowych w poufności? | |

| L.p. | PYTANIE | ODPOWIEDŹ |
|------|--|-----------|
| | <i>(Jeżeli odpowiedź jest twierdząca, proszę wskazać również w jakiej formie osoby te zostały zobowiązane do zachowania poufności: np. stosowne postanowienie o zachowaniu poufności danych osobowych w umowie o pracę.)</i> | |
| 33. | <p>Czy w przypadku przetwarzania Danych Osobowych na nośnikach elektronicznych (w szczególności dyskach twardych komputerów i na pendrive'ach) / optycznych ich zawartość jest/będzie szyfrowana?</p> <p><i>(Jeżeli odpowiedź na powyższe pytanie jest twierdząca, proszę wskazać jakim algorytmem (np. AES, Twofish, Serpent) i jakim kluczem (np. 128 bit, 192 bit, 256 bit) Dane Osobowe są/będą szyfrowane.)</i></p> | |
| 34. | W jaki sposób zabezpieczony jest dostęp do systemów informatycznych, w których przetwarzane są/będą Dane Osobowe (w szczególności czy PP stosuje: hasła, uwierzytelnianie dwu-/wieloskładnikowe, szyfrowanie danych, firewall, program antywirusowy)? | |
| 35. | W kontekście pytania z poprzedniej pozycji listy – jaka jest minimalna długość stosowanych haseł i ich złożoność/składnia i jak często są one zmieniane? | |
| 36. | Czy systemy/programy/aplikacje, w których przetwarzane są/będą Dane Osobowe odnotowują, kto i kiedy dane wprowadzał, zmieniał, usuwał? | |

| L.p. | PYTANIE | ODPOWIEDŹ |
|--|--|-----------|
| SEKCJA VI: NEGATYWNE DOŚWIADCZENIA PODMIOTU | | |
| 37. | <p>Czy PP (jako administrator lub podmiot przetwarzający) doświadczył naruszenia ochrony danych osobowych, dla którego konieczne było poinformowanie organu nadzorczego?</p> <p><i>(Jeżeli odpowiedź jest twierdząca, proszę również wskazać ile takich naruszeń miało miejsce w okresie ostatnich dwóch lat).</i></p> | |
| 38. | <p>Czy PP (jako administrator lub podmiot przetwarzający) doświadczył naruszenia ochrony danych osobowych, dla którego konieczne było poinformowanie osób, których ono dotyczyło?</p> <p><i>(Jeżeli odpowiedź jest twierdząca, proszę również wskazać ile takich naruszeń miało miejsce w okresie ostatnich dwóch lat).</i></p> | |
| 39. | <p>Czy stwierdzono prawomocną decyzją UODO/innego organu nadzorczego lub prawomocnym wyrokiem sądu naruszenie ochrony danych osobowych przez PP (działającego jako administrator lub podmiot przetwarzający)?</p> <p><i>(Jeśli odpowiedź jest twierdząca, proszę wskazać również dla wszystkich dotychczasowych naruszeń z okresu ostatnich dwóch lat: miesiąc i rok w którym nastąpiło naruszenie, podmiot, który wydał decyzję/wyrok oraz sygnaturę sprawy. Jeżeli</i></p> | |

| L.p. | PYTANIE | ODPOWIEDŹ |
|------|--|-----------|
| | <i><u>naruszenie miało miejsce przed dwoma laty proszę o zawarcie takiej informacji).</u></i> | |
| 40. | <p>W kontekście pytania z poprzedniej pozycji listy - czy UODO/organ nadzorczy nakazał/zalecił PP podjęcie określonych działań naprawczych?</p> <p><i><u>(Jeśli odpowiedź jest twierdząca, proszę wskazać czy te nakazy / zalecenia zostały w pełni zrealizowane).</u></i></p> | |

Oświadczam, że wszystkie informacje zawarte w niniejszej liście kontrolnej są zgodne z prawdą.

data: _____

podpis: _____
(imię i nazwisko osoby uprawnionej do reprezentowania Przetwarzającego)

KLAUZULA INFORMACYJNA

Niniejszą informację otrzymuje Pan/Pani w związku z obowiązkami określonymi w art. 13 i art. 14 rozporządzenia 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) (Dziennik Urzędowy Unii Europejskiej z dnia 4 maja 2016 r. L 119/1; dalej zwane również RODO).

1. Administrator (art. 13 ust. 1 lit. a oraz art. 14 ust. 1 lit. a RODO)

Administratorem Pana/Pani danych osobowych jest **Ekosystem spółka z ograniczoną odpowiedzialnością**.

adres siedziby: ul. Legnicka 51-53, 54-203 Wrocław
adres e-mail: ekosystem@ekosystem.wroc.pl
telefon: +48 71 758 69 11
NIP: 8992736747
nr w KRS: 0000426169

2. Inspektor ochrony danych (art. 13 ust. 1 lit. b oraz art. 14 ust. 1 lit. b RODO)

Administrator wyznaczył inspektora ochrony danych. Jest to osoba, z którą może się Pan/Pani kontaktować we wszystkich sprawach dotyczących: przetwarzania Pana/Pani danych osobowych oraz korzystania z przysługujących Panu/Pani praw związanych z przetwarzaniem tych danych.

Z inspektorem można kontaktować się:

pisemnie na adres: ul. Legnicka 51-53, 54-203 Wrocław,
poprzez e-mail: iodo@ekosystem.wroc.pl

3. Cele i podstawy prawne przetwarzania danych osobowych. Wskazanie prawnie uzasadnionego interesu realizowanego przez administratora lub osobę trzecią. Konieczność podania danych (art. 13 ust. 1 lit. c i d i ust. 2 lit. e oraz art. 14 ust. 1 lit. c i ust. 2 lit. b RODO)

Pana/Pani dane osobowe będą przetwarzane przez administratora w celu:

- 1) realizacji postanowień umowy (w tym w celach kontaktowych) zawartej przez administratora z Panem/Panią lub Pana/Pani pracodawcą / zleceniodawcą / zamawiającym / podmiotem, w którym odbywa Pan/Pani staż / praktykę albo który Pan/Pani reprezentuje (zwanymi dalej wspólnie „**Podmiotem Zatrudniającym**”); podstawę prawną przetwarzania Pani/Pana danych osobowych stanowi:
 - a. jeżeli umowa została zawarta z Panem/Panią – niezbędność przetwarzania danych osobowych dla realizacji umowy (art. 6 ust. 1 lit. b RODO),
 - b. jeżeli umowa została zawarta z Pana/Pani Podmiotem Zatrudniającym - uzasadniony interes prawny administratora (art. 6 ust. 1 lit. f RODO). Prawnie uzasadniony interes administratora wyraża się w tym przypadku koniecznością przetwarzania Pana/Pani danych osobowych na potrzeby prawidłowej realizacji ww. umowy;
 - c. niezbędność wykonania obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 lit. c oraz art. 9 ust. 1 lit. b RODO);
- 2) ustalenia, obrony i dochodzenia roszczeń; podstawą prawną przetwarzania Pana/Pani danych osobowych stanowi w tym wypadku uzasadniony interes prawny administratora (art. 6 ust. 1 lit. f oraz art. 9 ust. 1 lit. f RODO). Prawnie uzasadnionym interesem administratora jest w tym przypadku obrona przez szkodą majątkową

lub niemajątkową, albo rekompensata poniesionej szkody majątkowej lub niemajątkowej.

Jeżeli umowa została zawarta przez administratora z Panem/Panią, podanie Pana/Pani danych osobowych, które przetwarzane są w związku z realizacją:

- 1) umowy – jest dobrowolne, a ich niepodanie utrudni lub (wyjątkowo) uniemożliwi wykonanie umowy;
- 2) przez administratora obowiązków wynikających z przepisów prawa – jest obowiązkowe, a ich niepodanie uniemożliwi wykonanie umowy.

4. Kategorie odnośnych danych (art. 13 ust. 1 lit. d oraz art. 14 ust. 1 lit. d RODO)

Administrator będzie przetwarzał Pana/Pani służbowe dane kontaktowe (np. imię, nazwisko adres e-mail, telefon, dane komunikatora internetowego), które niezbędne są do należytej realizacji umowy zawartej przez administratora z: Panem/Panią lub Pana/Pani Podmiotem Zatrudniającym.

Jeżeli będzie Pan/Pani realizował na rzecz administratora świadczenia związane z wychowaniem, edukacją, wypoczynkiem, leczeniem, świadczeniem porad psychologicznych, rozwojem duchowym, uprawianiem sportu lub realizacją innych zainteresowań przez małoletnich, lub z opieką nad nimi, administrator będzie przetwarzał Pana/Pani dane zawarte w Rejestrze Sprawców Przestępstw na Tle Seksualnym oraz Krajowym Rejestrze Karnym, a jeżeli posiada Pan/Pani obywatelstwo innego Państwa niż Rzeczpospolita Polska albo/i w ciągu ostatnich 20 lat zamieszkiwał Pan/Pani na terenie innego kraju niż Rzeczpospolita Polska, również odpowiednio Pana/Pani dane osobowe z rejestru karnego państwa obywatelstwa albo/i z Pana/Pani oświadczenia o krajach miejsca zamieszkania w ostatnich 20 latach oraz z rejestrów krajów zamieszkania uzyskiwane do celów działalności zawodowej lub wolontariackiej związanej z kontaktami z dziećmi.

5. Odbiorcy danych osobowych (art. 13 ust. 1 lit. e oraz art. 14 ust. 1 lit. e RODO)

Odbiorcami Pani/Pana danych osobowych mogą być:

- 1) podmioty zapewniające administratorowi obsługę: informatyczną (w tym dostawca jego poczty elektronicznej), księgową lub prawną,
- 2) osoby korzystające z prawa dostępu do informacji publicznej lub informacji sektora publicznego;
- 3) inne podmioty upoważnione na podstawie przepisów prawa.

6. Przekazywanie danych do państwa trzeciego lub organizacji międzynarodowej (art. 13 ust. 1 lit. f oraz art. 14 ust. 1 lit. f RODO)

Pana/Pani dane osobowe mogą zostać przekazane do państwa trzeciego - tj. USA - przez podmiot świadczący dla administratora usługi poczty elektronicznej (gdyż m.in. tam znajdują się serwery tego podmiotu). W stosunku do USA Komisja Europejska stwierdziła odpowiedni poziom ochrony w ramach decyzji Data Privacy Framework, a podmiot świadczący usługi poczty elektronicznej dla administratora jest podmiotem certyfikowanym w ramach Data Privacy Framework.

7. Okres przechowywania Pana/Pani danych (art. 13 ust. 2 lit. a oraz art. 14 ust. 2 lit. a RODO)

Pani/Pana dane osobowe przetwarzane będą przez okres obowiązywania umowy zawartej pomiędzy administratorem a Panią/Panem lub Podmiotem Zatrudniającym, a następnie aż do upływu okresu przedawnienia roszczeń wynikających z tej umowy.

W zakresie Pani/Pana danych związanych z wychowaniem, edukacją, wypoczynkiem, leczeniem, świadczeniem porad psychologicznych, rozwojem duchowym, uprawianiem

sportu lub realizacją innych zainteresowań przez małoletnich, lub z opieką nad nimi, przez 5 lat od początku roku następującego po roku obrotowym, którego dotyczy dowód księgowy rozliczający umowę zawartą z administratorem przez Pana/Panią lub Pana/Pani Podmiot Zatrudniający.

8. Prawa osoby, której dane dotyczą, w tym prawo do cofnięcia zgody, jeżeli jest ona podstawą przetwarzania danych osobowych (art. 13 ust. 2 lit. b i c oraz art. 14 ust. 2 lit. c i d RODO)

Przysługują Panu/Pani następujące prawa związane z przetwarzaniem Pana/Pani danych osobowych: prawo dostępu do danych osobowych oraz prawo żądania ich sprostowania, usunięcia lub ograniczenia ich przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych.

Aby skorzystać z powyższych praw, proszę skontaktować się z administratorem lub inspektorem ochrony danych (dane kontaktowe powyżej w ust. 1 i 2).

9. Prawo wniesienia skargi do organu nadzorczego (art. 13 ust. 2 lit. d oraz 14 ust. 2 lit. e RODO)

Przysługuje Pani/Panu także prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych. W Polsce jest nim Prezes Urzędu Ochrony Danych Osobowych, ul. Stanisława Moniuszki 1A; 00-014 Warszawa.

10. Źródło pochodzenia danych (w tym źródeł publicznie dostępnych) (art. 14 ust. 2 lit. f RODO)

Pana/Pani dane osobowe pozyskane zostały od:

- 1) Pana/Pani Podmiotu Zatrudniającego w związku z Pana/Pani udziałem w realizacji umowy zawartej przez administratora z Pana/Pani Podmiotem Zatrudniającym,
- 2) w zakresie w jakim realizuje Pan/Pani świadczenia związane z wychowaniem, edukacją, wypoczynkiem, leczeniem, świadczeniem porad psychologicznych, rozwojem duchowym, uprawianiem sportu lub realizacją innych zainteresowań przez małoletnich, lub z opieką nad nimi – z rejestrów państwowych wymienionych w ust. 4 powyżej.

11. Informacja o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu (art. 13 ust. 2 lit. f oraz art. 14 ust. 2 lit. g RODO)

Pana/Pani dane osobowe nie będą wykorzystywane przez administratora do zautomatyzowanego podejmowania decyzji, w tym profilowania.