

**Porozumienie**  
**w sprawie powierzenia przetwarzania danych osobowych**

zwane dalej „**Porozumieniem**”,

zawarte pomiędzy:

**Ministrem Cyfryzacji** z siedzibą w Warszawie, ul. Królewska 27, 00-060 Warszawa, REGON: 525189465, NIP: 5252955037, zwanym dalej „**Ministrem Cyfryzacji**” lub „**MC**”, reprezentowanym przez Pana Krzysztofa Karakulę Dyrektora Departamentu Transformacji Cyfrowej w Ministerstwie Cyfryzacji, na podstawie upoważnienia DP.MC.WPP.0103.55.2024 z dnia 07 lutego 2024 r., zwanym dalej „**Podmiotem przetwarzającym**”

a

Polską Izbą Inżynierów Budownictwa z siedzibą w Warszawie, ul. Kujawska 1, 00-793 Warszawa NIP: 5252254990, REGON: 015314008 reprezentowanym przez: Krajową Radę w imieniu której działają:

Pan mgr inż. Mariusz Dobrzeniecki – Prezes Krajowej Rady Polskiej Izby Inżynierów Budownictwa,

Pani mgr inż. Elżbieta Bryła- Kluczny - Skarbnik Krajowej Rady Polskiej Izby Inżynierów Budownictwa, zwanym dalej „**Administratorem**”,

zwanymi dalej łącznie „**Stronami**”, a każdy z osobna „**Stroną**”.

**§ 1. Przedmiot porozumienia**

1. Administrator i Podmiot przetwarzający zawierają porozumienie w sprawie powierzenia przetwarzania danych osobowych, zwane dalej „Porozumieniem”, na mocy której Administrator powierza w trybie art. 28 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), zwanego dalej „**RODO**”, Podmiotowi przetwarzającemu przetwarzanie danych osobowych, rozumianych jako informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą), które są zgromadzone w rejestrach, ewidencjach, zbiorach, systemach teleinformatycznych i aplikacjach pozostających we właściwości Administratora, zwanych dalej „**Danymi osobowymi**”, w celu realizacji **Porozumienia w sprawie zakresu i warunków opracowania, udostępnienia, wdrożenia i umożliwienia świadczenia w aplikacji mObywatel usługi prezentowania i obsługi dokumentu „Legitymacja inżyniera budownictwa”**, zwanemu dalej „**Porozumieniem Głównym**”.
2. Rodzaj Danych osobowych, ich zakres oraz kategorie osób, których dane dotyczą, które Administrator powierza Podmiotowi przetwarzającemu na potrzeby realizacji Porozumienia Głównego określa **załącznik nr 1 do Porozumienia**.
3. Powierzenie Danych osobowych Podmiotowi przetwarzającemu następuje wyłącznie w celu wykonania Porozumienia Głównego.
4. Określa się następujący charakter przetwarzania Danych osobowych przez Podmiot przetwarzający: 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 ich niszczenie.
5. Podmiot przetwarzający może przetwarzać Dane osobowe wyłącznie w zakresie i celu określonym w Porozumieniu oraz w celu i zakresie niezbędnym do wykonywania przez Podmiot przetwarzający powierzonych zadań określonych w Porozumieniu Głównym. Przetwarzanie Danych osobowych przez Podmiot przetwarzający odbywa się wyłącznie w czasie obowiązywania Porozumienia Głównego.

**§ 2. Oświadczenia i obowiązki podmiotu przetwarzającego**

1. Podmiot przetwarzający jest zobowiązany:

- 1) przetwarzać Dane osobowe zgodnie z RODO, polskimi przepisami przyjętymi w celu umożliwienia stosowania RODO, innymi obowiązującymi przepisami prawa, Porozumieniem oraz instrukcjami lub poleceniami Administratora. Instrukcje lub polecenia są przekazywane przez Administratora drogą elektroniczną na adres poczty elektronicznej **koordynatora Porozumienia** wyznaczonego przez Podmiot przetwarzający, z zastrzeżeniem postanowień § 3, Podmiot przetwarzający powinien wdrożyć instrukcje lub polecenia niezwłocznie, jednak nie później niż w terminie 7 dni roboczych od ich otrzymania; jeżeli w ocenie Podmiotu przetwarzającego termin 7-dniowy jest zbyt krótki na realizację instrukcji lub polecenia, powinien poinformować o tym fakcie Administratora drogą elektroniczną na adres poczty elektronicznej koordynatora Porozumienia wyznaczonego przez Administratora wskazując uzasadnienie dla takiej oceny; w takim przypadku Strony wspólnie ustalą późniejszy termin wdrożenia instrukcji lub polecenia Administratora. Instrukcje lub polecenia nie będą rozszerzać zakresu obowiązków Podmiotu przetwarzającego wynikających z Porozumienia ani Porozumienia Głównego;
- 2) przetwarzać Dane osobowe wyłącznie na udokumentowane polecenie Administratora, chyba że obowiązek taki nakłada na niego obowiązujące prawo krajowe lub unijne. W sytuacji, gdy obowiązek przetwarzania danych osobowych przez Podmiot przetwarzający wynika z przepisów prawa, informuje on Administratora drogą elektroniczną na adres poczty elektronicznej koordynatora Porozumienia wyznaczonego przez Administratora – przed rozpoczęciem przetwarzania - o tym obowiązku prawnym, o ile prawo nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;
- 3) przetwarzać Dane osobowe wyłącznie w miejscu ustalonym w Porozumieniu oraz na urządzeniach zarządzanych przez Podmiot przetwarzający lub Administratora, z zachowaniem najwyższych zasad bezpieczeństwa i ochrony danych osobowych wymaganych przez obowiązujące przepisy prawa;
- 4) udzielać dostępu do Danych osobowych wyłącznie osobom, które ze względu na zakres wykonywanych zadań otrzymały od Podmiotu przetwarzającego upoważnienie do ich przetwarzania oraz wyłącznie w celu wykonywania obowiązków wynikających z Porozumienia oraz podjąć działania mające na celu zapewnienie, by każda osoba fizyczna działająca z upoważnienia Podmiotu przetwarzającego, która ma dostęp do Danych osobowych, przetwarzała je wyłącznie na polecenie Administratora, chyba że przetwarzanie jest wymagane przez właściwe przepisy krajowe lub unijne;
- 5) zapewnić, aby osoby upoważnione do przetwarzania Danych osobowych zobowiązały się do zachowania tajemnicy, chyba że są to osoby podlegające odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
- 6) wdrożyć, zgodnie z wytycznymi wskazanymi w § 3 Porozumienia, odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych, których Dane osobowe będą przetwarzane na podstawie Porozumienia oraz zapewnić realizację zasad ochrony danych w fazie projektowania oraz domyślnej ochrony danych, określonych w art. 25 RODO;
- 7) wspierać Administratora, w szczególności poprzez stosowanie odpowiednich środków technicznych i organizacyjnych, w realizacji obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw określonych w rozdziale III RODO. Współpraca Podmiotu przetwarzającego z Administratorem, w zakresie wskazanym w zdaniu poprzedzającym, powinna odbywać się w formie i terminie umożliwiającym realizację tych obowiązków Administratora; w związku z realizacją tego obowiązku Podmiot przetwarzający jest w szczególności zobowiązany do udzielania informacji oraz ujawnienia powierzonych danych osobowych lub ich kopii na żądanie Administratora w terminie 5 dni roboczych w formie określonej przez Administratora; Podmiot przetwarzający powinien również niezwłocznie, jednak nie później niż w terminie 2 dni roboczych, poinformować Administratora o wniosku dotyczącym realizacji praw osoby, której dane dotyczą, złożonym u Podmiotu przetwarzającego;
- 8) pomagać Administratorowi wywiązać się z obowiązków określonych w RODO art. 32-36 RODO, w szczególności w zakresie:

- a) zapewnienia bezpieczeństwa przetwarzania Danych osobowych poprzez wdrożenie stosownych środków technicznych oraz organizacyjnych; wykaz minimalnych środków, które zobowiązany jest wdrożyć Podmiot przetwarzający określa **załącznik nr 3 do Porozumienia**;
  - b) dokonywania zgłaszania naruszeń ochrony danych osobowych organowi nadzorczemu w rozumieniu art. 4 pkt. 21 RODO oraz zawiadamiania osób, których dane dotyczą o takim naruszeniu; obowiązki Podmiotu przetwarzającego w odniesieniu do zgłaszania naruszeń zostały określone w § 7 Porozumienia;
  - c) dokonywania przez Administratora oceny skutków dla ochrony danych osobowych oraz wsparcia Administratora w przeprowadzaniu konsultacji z organem nadzorczym. Strony będą uzgadniać szczegółowy sposób i tryb wykonywania oceny skutków dla ochrony danych osobowych w ramach wykonywania Porozumienia Głównego;
  - d) realizacja procesów i wymagań określonych w przepisach rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247, z późn. zm.);
- 9) prowadzić, w formie pisemnej albo elektronicznej, rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora, zawierający informacje o:
- a) nazwie oraz danych kontaktowych Podmiotu przetwarzającego oraz Administratora, a także inspektora ochrony danych, gdy ma to zastosowanie;
  - b) kategoriach przetwarzania dokonywanych w imieniu Administratora;
  - c) gdy ma to zastosowanie – przekazywaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwie tego państwa trzeciego lub organizacji międzynarodowej, zgodnie i na zasadach określonych w § 5;
  - d) ogólnym opisie technicznych i organizacyjnych środków bezpieczeństwa, służących do zabezpieczenia powierzonych danych osobowych;
- 10) udostępniać Administratorowi, na każde jego żądanie, nie później niż w terminie 5 dni roboczych, wszelkie informacje niezbędne do wykazania spełnienia przez Administratora obowiązków wynikających z właściwych przepisów prawa, w szczególności z RODO, w tym przekazywać informacje o stosowanych zabezpieczeniach, zidentyfikowanych zagrożeniach i incydentach w obszarze ochrony danych osobowych;
- 11) umożliwiać Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów na zasadach określonych w § 6 Porozumienia;
- 12) niezwłocznie informować Administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie RODO lub innych przepisów krajowych lub unijnych o ochronie danych osobowych; informacja w tym przedmiocie przekazana powinna zostać Administratorowi drogą elektroniczną na adres poczty elektronicznej **koordynatora Porozumienia** wyznaczonego przez Administratora oraz powinna zawierać stosowne uzasadnienie i wskazanie przepisu prawa, który zdaniem Podmiotu przetwarzającego został naruszony;
- 13) niezwłocznie, jednak nie później niż w ciągu 2 dni roboczych, informować, o ile nie doprowadzi to do naruszenia przepisów obowiązującego prawa, Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania Danych osobowych przez Podmiot przetwarzający, o jakiegokolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania Danych osobowych, skierowanej do Podmiotu przetwarzającego, o wszelkich kontrolach i inspekcjach dotyczących przetwarzania Danych osobowych przez Podmiot przetwarzający, w szczególności prowadzonych przez organ nadzorczy a także o wszelkich skargach osób, których dane dotyczą związanych z przetwarzaniem ich danych osobowych;
- 14) przechowywać Dane osobowe tylko tak długo, jak to określił Administrator, a także, bez zbędnej zwłoki, aktualizować, poprawiać, zmieniać, anonimizować, ograniczać przetwarzanie lub usuwać wskazane Dane osobowe zgodnie z wytycznymi Administratora i Porozumieniem Głównym.

2. Dla celów wykonania zobowiązań wskazanych w § 2 ust. 1 pkt 4 i 5, Strony potwierdzają, że Podmiot przetwarzający jest uprawniony do nadawania i odwoływania upoważnień pracownikom Podmiotu przetwarzającego, osobom współpracującym z Podmiotem przetwarzającym na podstawie umów cywilnoprawnych, podwykonawcom Podmiotu przetwarzającego, do przetwarzania Danych osobowych powierzonych do przetwarzania na podstawie Porozumienia, według wzorów dokumentów obowiązujących u Podmiotu przetwarzającego.

### § 3. Środki organizacyjne i techniczne

1. Podmiot przetwarzający wdraża i stosuje adekwatne środki techniczne i organizacyjne, w celu zapewnienia stopnia bezpieczeństwa odpowiedniego do ryzyka naruszenia praw lub wolności osób fizycznych, których Dane osobowe są przetwarzane na podstawie Porozumienia.
2. Oceniając, czy stopień bezpieczeństwa, o którym mowa w § 3 ust. 1, jest odpowiedni, Podmiot przetwarzający jest zobowiązany uwzględnić ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do Danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
3. Podmiot przetwarzający powinien również wdrożyć odpowiednie środki techniczne i organizacyjne, zaprojektowane w celu skutecznej realizacji zasad ochrony danych określonych w RODO oraz w celu ochrony praw osób, których dane dotyczą (zasada ochrony danych osobowych w fazie projektowania określona w art. 25 ust. 1 RODO), a także odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia celu przetwarzania określonego w Porozumieniu (zasada domyślnej ochrony danych określona w art. 25 ust. 2 RODO).
4. Wdrażając środki organizacyjne i techniczne, o których mowa powyżej, Podmiot przetwarzający:
  - 1) przestrzega wytycznych Administratora w zakresie sposobu zabezpieczenia procesów przetwarzania Danych osobowych zgodnie z przepisami obowiązującego prawa;
  - 2) powinien uwzględnić stan wiedzy technicznej oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych, których Dane osobowe będzie przetwarzał na podstawie Porozumienia.
5. W przypadku stwierdzenia, że stosowane środki mogą być nieadekwatne do rozpoznanych zagrożeń, Podmiot przetwarzający informuje o tym Administratora i w porozumieniu z Administratorem dostosowuje odpowiednio zabezpieczenia przetwarzania Danych osobowych, po uzgodnieniu przez Strony zakresu, sposobu i terminu takich działań.. Związane z tym koszty ponoszone będą na zasadach określonych w Porozumieniu Głównym.

### § 4. Dalsze powierzenie przetwarzania

1. Administrator wyraża zgodę na dalsze powierzenie przez Podmiot przetwarzający przetwarzania Danych osobowych innym podmiotom przetwarzającym wskazanym **w załączniku nr 2 do Porozumienia** w zakresie oraz celu zgodnym z Porozumieniem. Podmiot przetwarzający jest zobowiązany do informowania drogą elektroniczną na adres poczty elektronicznej koordynatora Porozumienia wyznaczonego przez Administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia dalszych podmiotów przetwarzających. Administrator może sprzeciwić się dalszemu powierzeniu przez Podmiot przetwarzający Danych osobowych, w terminie 7 dni roboczych od otrzymania informacji, o której mowa w zdaniu poprzedzającym. W przypadku wyrażenia sprzeciwu przez Administratora, Podmiot przetwarzający nie jest uprawniony do powierzenia przetwarzania Danych osobowych dalszemu podmiotowi przetwarzającemu, którego dotyczy sprzeciw.
2. Podmiot przetwarzający zapewnia, że będzie korzystał wyłącznie z usług takich dalszych podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO oraz przepisów obowiązującego prawa z zakresu ochrony danych osobowych, wskazanych w § 2 ust. 1 pkt 1, a także zapewniało ochronę praw osób, których dane dotyczą.

3. Podmiot przetwarzający zapewni w umowie z dalszym podmiotem przetwarzającym, zawarcie umowy na piśmie, zgodnej z celami i warunkami niniejszego Porozumienia oraz, że na podmiot ten zostaną nałożone obowiązki odpowiadające obowiązkom Podmiotu przetwarzającego określone w Porozumieniu, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom RODO.
4. Podmiot przetwarzający zapewni również w umowie z dalszym podmiotem przetwarzającym możliwość realizacji przez Administratora bezpośredniej kontroli względem dalszego podmiotu przetwarzającego, w tym możliwość przeprowadzania audytów, o których mowa w § 6 Porozumienia. Podmiot przetwarzający jest zobowiązany poinformować dalszy podmiot przetwarzający, że informacje, w tym dane osobowe, na temat tego podmiotu przetwarzającego mogą być udostępnione Administratorowi w celu wykonania przez niego uprawnień, o których mowa w zdaniu poprzedzającym.
5. Podmiot przetwarzający jest w pełni odpowiedzialny przed Administratorem za spełnienie obowiązków wynikających z umowy powierzenia zawartej pomiędzy Podmiotem przetwarzającym a dalszym podmiotem przetwarzającym. Jeżeli dalszy podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych osobowych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków tego dalszego podmiotu przetwarzającego spoczywa na Podmiocie przetwarzającym.
6. Podmiot przetwarzający zobowiązany jest podjąć kroki, aby zapewnić, by dalszy podmiot przetwarzający zaprzestał przetwarzania Danych osobowych w każdym wypadku rozwiązania Porozumienia, niezależnie od przyczyny oraz w przypadku upływu okresu przetwarzania Danych osobowych na podstawie Porozumienia Głównego.

#### **§ 5. Transfer danych osobowych**

Podmiot przetwarzający nie może przekazywać (transferować) Danych osobowych do państwa trzeciego, które znajduje się poza Europejskim Obszarem Gospodarczym, chyba że Administrator udzieli mu uprzedniej, pisemnej pod rygorem bezskuteczności, zgody zezwalającej na taki transfer. Jeśli Administrator udzieli Podmiotowi przetwarzającemu uprzedniej zgody na przekazanie Danych osobowych do państwa trzeciego, które znajduje się poza Europejskim Obszarem Gospodarczym, Podmiot przetwarzający może dokonać transferu tych Danych osobowych tylko wtedy, gdy:

- 1) państwo docelowe zapewnia adekwatny poziom ochrony danych osobowych do tego, który obowiązuje w Unii Europejskiej; lub
- 2) Administrator i Podmiot przetwarzający lub dalszy podmiot przetwarzający zawarli umowę w oparciu o standardowe klauzule umowne lub wdrożyli inny mechanizm, który zgodnie z przepisami prawa legalizuje transfer danych osobowych do państwa trzeciego.

#### **§ 6. Audyt**

1. Administrator jest w każdym momencie upoważniony do przeprowadzenia audytu zgodności przetwarzania Danych osobowych przez Podmiot przetwarzający z Porozumieniem oraz obowiązującymi przepisami prawa, w szczególności Administrator może przeprowadzić weryfikację zgodności i adekwatności środków technicznych i organizacyjnych zabezpieczających przetwarzanie Danych osobowych wdrożonych przez Podmiot przetwarzający.
2. Administrator informuje Podmiot przetwarzający co najmniej na 3 dni robocze przed planowaną datą audytu o zamiarze jego przeprowadzenia, chyba że z uwagi na wysokie ryzyko zagrożenia praw i wolności osób, których dane dotyczą, audyt powinien być przeprowadzony niezwłocznie. Jeżeli w ocenie Podmiotu przetwarzającego audyt nie może zostać przeprowadzony we wskazanym terminie Podmiot przetwarzający powinien poinformować o tym fakcie Administratora drogą elektroniczną na adres poczty elektronicznej koordynatora Porozumienia wyznaczonego przez Administratora) wskazując uzasadnienie dla takiej oceny. W takim przypadku Strony wspólnie ustalą późniejszy termin audytu.

3. Podmiot przetwarzający ma obowiązek współpracować z Administratorem i upoważnionymi przez niego audytorami, w szczególności zapewniać im dostęp do pomieszczeń i dokumentów obejmujących Dane osobowe oraz informacje o sposobie przetwarzania Danych osobowych, infrastruktury teleinformatycznej oraz systemów IT, a także do osób mających wiedzę na temat procesów przetwarzania Danych osobowych realizowanych przez Podmiot przetwarzający. W przypadku gdy wdrożenie tych zaleceń będzie wiązać się z dodatkowymi kosztami, Strony wspólnie ustalą sposób ich ponoszenia przez Strony.
4. Administrator ma także prawo żądać od Podmiotu przetwarzającego składania pisemnych wyjaśnień dotyczących realizacji Umowy. Podmiot przetwarzający zobowiązuje się odpowiedzieć niezwłocznie, jednak nie później niż w terminie 3 dni roboczych, na każde pytanie Administratora dotyczące przetwarzania powierzonych mu na podstawie Porozumienia Danych osobowych.
5. Podmiot przetwarzający jest zobowiązany zapewnić w umowie z dalszym podmiotem przetwarzającym możliwość przeprowadzania przez Administratora audytu zgodności przetwarzania Danych osobowych przez dalszy podmiot przetwarzający z Porozumieniem na zasadach określonych w ust. 1-4.
6. Koszty związane z przeprowadzeniem audytu ponosi każda ze Stron we własnym zakresie, przy czym Podmiot przetwarzający nie ma prawa do żądania od Administratora zwrotu takich kosztów ani zapłaty jakiegokolwiek dodatkowego wynagrodzenia z tytułu poniesienia takich kosztów, o ile ich ponoszenie przez podmiot przetwarzający wynika z zaniechań leżących po jego stronie.

## **§ 7. Zgłaszanie naruszeń**

1. Podmiot przetwarzający jest zobowiązany do wdrożenia i stosowania procedur służących wykrywaniu naruszeń ochrony Danych osobowych oraz wdrażaniu właściwych środków naprawczych.
2. Po stwierdzeniu naruszenia ochrony powierzonych mu przez Administratora Danych osobowych Podmiot przetwarzający, bez zbędnej zwłoki, jednak nie później niż w ciągu 24 godzin od stwierdzenia naruszenia, zgłasza je Administratorowi na adres poczty elektronicznej **iod@piib.org.pl**. Zgłoszenie powinno zawierać co najmniej informacje o:
  - 1) dacie, czasie trwania oraz lokalizacji naruszenia ochrony Danych osobowych;
  - 2) charakterze i skali naruszenia, tj. w szczególności o kategoriach i przybliżonej liczbie osób, których dane dotyczą, oraz kategoriach i przybliżonej liczbie wpisów Danych osobowych, których dotyczy naruszenie;
  - 3) systemie informatycznym, w którym wystąpiło naruszenie (jeżeli naruszenie nastąpiło w związku z przetwarzaniem Danych osobowych w systemie informatycznym);
  - 4) przewidywanym czasie potrzebnym do naprawienia szkody spowodowanej naruszeniem;
  - 5) charakterze i zakresie Danych osobowych objętych naruszeniem;
  - 6) kategoriach osób, których dotyczą Dane osobowe objęte naruszeniem, a w razie możliwości także wskazania podmiotów danych, których dotyczyło naruszenie;
  - 7) możliwych konsekwencjach naruszenia, z uwzględnieniem konsekwencji dla osób, których dane dotyczą;
  - 8) środkach podjętych w celu zminimalizowania konsekwencji naruszenia oraz proponowanych działaniach zapobiegawczych i naprawczych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków;
  - 9) danych kontaktowych osoby mogącej udzielić dalszych informacji o naruszeniu.
3. Jeżeli Podmiot przetwarzający nie jest w stanie w tym samym czasie przekazać Administratorowi wszystkich informacji, o których mowa powyżej, powinien je udzielać sukcesywnie, bez zbędnej zwłoki.
4. Podmiot przetwarzający bez zbędnej zwłoki podejmuje wszelkie rozsądne działania mające na celu ograniczenie i naprawienie negatywnych skutków naruszenia.

5. Podmiot przetwarzający jest zobowiązany do dokumentowania wszelkich naruszeń ochrony powierzonych mu Danych osobowych, w tym okoliczności naruszenia ochrony Danych osobowych, jego skutków oraz podjętych działań zaradczych. Podmiot przetwarzający jest zobowiązany na każde żądanie Administratora niezwłocznie udostępnić mu dokumentację, o której mowa w zdaniu poprzednim.

#### **§ 8. Czas trwania przetwarzania oraz zasady odpowiedzialności**

1. Administrator powierza Podmiotowi przetwarzającemu przetwarzanie Danych osobowych na czas obowiązywania Porozumienia w zakresie określonym w § 1 ust. 2 Porozumienia.
2. Administrator uprawniony jest do wypowiedzenia Porozumienia ze skutkiem natychmiastowym w przypadku zaistnienia ważnych powodów, w tym także w razie naruszenia przez Podmiot przetwarzający lub dalszy podmiot przetwarzający przepisów RODO, innych obowiązujących przepisów prawa lub Porozumienia, a w szczególności, gdy:
  - 1) organ nadzoru nad przestrzeganiem zasad przetwarzania danych osobowych stwierdzi, że Podmiot przetwarzający lub dalszy podmiot przetwarzający nie przestrzega zasad przetwarzania danych osobowych,
  - 2) prawomocne orzeczenie sądu powszechnego wykaże, że Podmiot przetwarzający nie przestrzega zasad przetwarzania danych osobowych;
  - 3) Administrator, w wyniku przeprowadzenia audytu, o którym mowa w § 6 Porozumienia stwierdzi, że Podmiot przetwarzający nie przestrzega zasad przetwarzania Danych osobowych wynikających z Porozumienia lub obowiązujących przepisów prawa oraz Podmiot przetwarzający nie zastosował się do zaleceń pokontrolnych.
3. Naruszenie przez Podmiot przetwarzający postanowień Porozumienia, RODO lub innych obowiązujących przepisów prawa z zakresu ochrony danych osobowych stanowi podstawę do wypowiedzenia Porozumienia Głównego.
4. W dniu zakończenia obowiązywania Porozumienia Podmiot przetwarzający powinien zgodnie z dyspozycją Administratora zwrócić lub zniszczyć, w sposób odrębnie ustalony z Administratorem, wszelkie Dane osobowe i ich kopie, chyba że właściwe przepisy prawa krajowego lub unijnego nakazują przechowywanie tych Danych osobowych.
5. Na prośbę Administratora, Podmiot przetwarzający przesyła pisemne potwierdzenie zniszczenia Danych osobowych w terminie przez niego wskazanym.
6. W przypadku ograniczenia zakresu powierzenia przetwarzania przez Administratora, w trybie określonym w Porozumieniu postanowienia o rozwiązaniu Porozumienia stosuje się odpowiednio do danych, które wskutek ograniczenia zakresu nie mogą już być przetwarzane przez Podmiot przetwarzający.
7. W przypadku dalszego powierzenia przetwarzania Danych osobowych Podmiot przetwarzający zobowiązuje się do zawarcia w umowach z dalszymi podmiotami przetwarzającymi postanowień, zgodnie z którymi dalszy podmiot przetwarzający zaprzestanie przetwarzania powierzonych Danych osobowych w każdym wypadku rozwiązania /Porozumienia Głównego z dniem rozwiązania oraz w przypadku upływu okresu przetwarzania danych w Porozumieniu Głównym, o którym mowa w § 8 ust. 1. W takim przypadku postanowienia § 8 ust. 4 i 5 stosuje się odpowiednio.
8. Podmiot przetwarzający odpowiada za szkody, jakie powstaną u Administratora, osób, których dane dotyczą lub innych osób trzecich w wyniku niezgodnego z Porozumieniem, porozumieniem lub umową z dalszym podmiotem przetwarzającym lub przepisami prawa, przetwarzania przez dalszy podmiot przetwarzający, a w szczególności w związku z udostępnianiem Danych osobowych osobom nieuprawnionym lub nieupoważnionym.
9. Podmiot przetwarzający ponosi względem Administratora odpowiedzialność na zasadach ogólnych. Zasady odpowiedzialności określone w niniejszym Porozumieniu nie wyłączają odpowiedzialności Stron określonej zgodnie z obowiązującymi przepisami prawa, w szczególności art. 83 RODO.

### **§ 9. Adresy stron i dane osób**

1. Podejmowanie decyzji oraz bieżące zarządzanie realizacją Porozumienia odbywać się będzie przez wzajemne uzgodnienia koordynatorów Porozumienia. Koordynatorzy Porozumienia będą uprawnieni w szczególności do dokonywania zmian w załącznikach do Porozumienia, przy czym zmiany załączników nie będą uważane za zmiany Porozumienia i nie będą wymagały zawarcia aneksu do Porozumienia.
2. Strony ustanawiają następujących koordynatorów Porozumienia:
  - 1) ze strony Administratora:

Krzysztof Zając;  
adres poczty elektronicznej: [iod@piib.org.pl](mailto:iod@piib.org.pl) ;  
tel. +48 22 8933010
  - 2) ze strony Podmiotu przetwarzającego:

Krzysztof Karakula; adres poczty elektronicznej: [Krzysztof.Karakula@cyfra.gov.pl](mailto:Krzysztof.Karakula@cyfra.gov.pl);  
tel. +48 723 997 933;
3. Zmiana danych, o których mowa w ust. 2, nie wymaga zawarcia aneksu do Porozumienia, lecz staje się skuteczna z dniem doręczenia drugiej Stronie, oświadczenia w postaci elektronicznej opatrzonej podpisem zaufanym, podpisem osobistym lub kwalifikowanym podpisem elektronicznym.

### **§ 10. Postanowienia końcowe**

1. Porozumienie zostaje zawarte w postaci elektronicznej i wymaga opatrzenia podpisem zaufanym, podpisem osobistym lub kwalifikowanym podpisem elektronicznym pod rygorem nieważności.
2. Wszystkie zmiany Porozumienia wymagają postaci elektronicznej i wymagają opatrzenia podpisem zaufanym, podpisem osobistym lub kwalifikowanym podpisem elektronicznym pod rygorem nieważności, z zastrzeżeniem § 9 ust. 1.
3. Integralną część Porozumienia stanowią:
  - 1) załącznik nr 1 - Zakres powierzenia przetwarzania
  - 2) załącznik nr 2 - Lista dalszych podmiotów przetwarzających ;
  - 3) załącznik nr 3 - Wykaz minimalnych środków technicznych i organizacyjnych, które zobowiązany jest wdrożyć Podmiot przetwarzający.
4. Porozumienie wchodzi w życie z dniem podpisania przez ostatnią ze Stron

Administrator

Podmiot przetwarzający



## **Załącznik nr 1**

### **Zakres powierzenia przetwarzania**

- 1) Numer PESEL;
- 2) Nazwa Podmiotu (właściwa Okręgowa Izba Inżynierów Budownictwa);
- 3) Numer członkowski;
- 4) Data ważności zaświadczenia o przynależności do Izby;
- 5) Informacja o posiadaniu wymaganego ubezpieczenia OC.

## **Załącznik nr 2**

### **Lista dalszych podmiotów przetwarzających**

Centralny Ośrodek Informatyki z siedzibą w Warszawie, Aleje Jerozolimskie 132-136, 02-305 Warszawa, wpisany do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000372110, NIP: 725-203-68-63, REGON: 100-999-489

**Pan Wojciech Stańczuk, prowadzący działalność gospodarczą pod nazwą „Wojciech Stańczuk ENTIM”, adres do doręczeń: ul. Michała Kleofasa Ogińskiego, nr 24, lok. 24, 03345 Warszawa, NIP 1251113788, REGON 140135823**

**e-MSI Sp. z o.o.** z siedzibą w Poznaniu, przy ul. Stablewskiego 47/2N, 60-213 Poznań, wpisaną do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy Poznań – Nowe Miasto i Wilda w Poznaniu, IX Wydział Gospodarczy KRS pod numerem 0000387940, numer NIP: 7881989611, REGON: 30755665

### Załącznik nr 3

#### **Wykaz minimalnych środków technicznych i organizacyjnych, które zobowiązany jest wdrożyć Podmiot przetwarzający**

W celu zapewnienia odpowiedniego stopnia zabezpieczenia powierzonych danych Podmiot przetwarzający jest zobowiązany wdrożyć co najmniej następujące środki techniczne i organizacyjne:

- 1) zastosować następujące techniki pseudonimizacji: szyfrowanie kluczem tajnym, tokenizacja, zastosowanie funkcji skrótu;
- 2) zastosować następujące metody szyfrowania danych osobowych: pseudonimizacja, kryptografia symetryczna, kryptografia asymetryczna, techniki anonimizacji;
- 3) zapewnić możliwość ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów służących do przetwarzania danych osobowych oraz usług przetwarzania;
- 4) zapewnić możliwość szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
- 5) dokonywać regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych;
- 6) zapewnić mechanizmy kontroli dostępu do systemu informatycznego w którym przetwarza się dane osobowe, w taki sposób, że dostęp do tych danych byłby możliwie jedynie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia;
- 7) zapewnić ochronę systemów informatycznych służących do przetwarzania danych osobowych w szczególności przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego oraz przed utratą danych spowodowaną awarią zasilania lub zakłócenia w sieci zasilającej;
- 8) zapewnić bezpieczeństwo danych osobowych w systemie informatycznym przez wykonywanie kopii zapasowej zbiorów danych oraz programów służących do przetwarzania danych. Kopie zapasowe należy przechowywać w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem, lub zniszczeniem oraz usuwa się je niezwłocznie po ustaniu ich użyteczności;
- 9) zapewnić by urządzenia, dyski, lub inne nośniki elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do likwidacji lub przekazania podmiotowi nieuprawnionemu pozbawić wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkodzić w sposób uniemożliwiający ich odzyskanie lub/i odczytanie;
- 10) zapewnić ochronę systemów informatycznych służących do przetwarzania danych osobowych przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem;
- 11) zapewnić środki kryptograficzne ochrony wobec danych wykorzystywanych do uwierzytelniania, które są przesyłane w sieci publicznej.