PROCEDURA WYBORU
PODMIOTU PRZETWARZAJĄCEGO
DANE OSOBOWE

1. POSTANOWIENIA OGÓLNE

1.1. Niniejsza Procedura określa sposób przeprowadzenia procesu wyboru Dostawców, którym Spółka powierza przetwarzanie Danych osobowych.

1.2. Pojęcia pisane wielką literą mają znaczenie zdefiniowane poniżej:

1.2.1. **Administrator** lub **Spółka** – dana spółka z grupy CRH w Polsce.

1.2.2. **Dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak: imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość tej osoby.

1.2.3. **Dostawca** – osoba fizyczna prowadząca działalność gospodarczą lub jednostka organizacyjna posiadająca osobowość prawną lub nieposiadająca osobowości prawnej (niezależnie od tego, czy taka jednostka jest członkiem grupy kapitałowej, do której należy Spółka), która na podstawie umowy zawartej ze Spółką dotyczącej korzystania przez Spółkę z Usług przetwarza Dane osobowe, których Spółka jest administratorem lub w stosunku do których Spółka jest podmiotem przetwarzającym Dane osobowe na zlecenie administratora.

1.2.4. **EOG** – Europejski Obszar Gospodarczy obejmujący kraje UE oraz Islandię, Norwegię i Liechtenstein.

1.2.5. **Koordynator ds. ochrony danych osobowych (KODO)** – osoba wskazana przez Administratora wspierająca go w zakresie koordynowania i wykonywania zadań związanych z zapewnieniem zgodności przetwarzania danych osobowych w Spółce z obowiązującym prawem.

1.2.6. **Kandydat na Dostawcę** – podmiot, z którym Spółka rozważa zawarcie Umowy lub który zostaje poddany weryfikacji zgodnie z Procedurą.

1.2.7. **Podmiot Danych** – osoba, której dotyczą Dane osobowe przetwarzane przez Spółkę.

1.2.8. **Procedura** – niniejsza Procedura wyboru Dostawcy – podmiotu przetwarzającego Dane osobowe na zlecenie Spółki.

1.2.9. **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).

1.2.10. **Szczególne Kategorie Danych** – Dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności albo orientacji seksualnej tej osoby.

1.2.11. **Umowa** – umowa pomiędzy Spółką a Dostawcą, w ramach wykonania której Dostawca przetwarza Dane osobowe pochodzące od Spółki.

1.2.12. **Umowa Powierzenia** – umowa powierzenia przetwarzania Danych osobowych lub umowa dalszego powierzenia przetwarzania Danych osobowych, która ma zostać zawarta pomiędzy Spółką a Dostawcą w związku z Umową.

1.2.13. **Usługi** – usługi lub inne świadczenia wykonywane przez Dostawcę na rzecz Spółki, z którymi wiąże się przetwarzanie przez Dostawcę Danych osobowych pochodzących od Spółki.

2. WARUNKI DOPUSZCZALNOŚCI ZAWARCIA UMOWY POWIERZENIA Z DOSTAWCĄ

2.1. Warunkiem dopuszczalności powierzenia przetwarzania Danych osobowych jest zapewnienie przez kandydata na Dostawcę gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, tak by przetwarzanie spełniało wymogi wskazane w RODO i chroniło prawa Podmiotów Danych.

2.2. Spółka może powierzyć Kandydatowi na Dostawcę przetwarzanie Danych osobowych na podstawie Umowy Powierzenia, gdy kandydat na Dostawcę przeszedł pozytywną weryfikację zgodnie z rozdziałem 3 Procedury „Weryfikacja kandydata na Dostawcę".

2.3. Weryfikacja Kandydata na Dostawcę powinna zostać przeprowadzona przez zawarciem Umowy oraz Umowy Powierzenia.

3. WERYFIKACJA KANDYDATA NA DOSTAWCĘ

3.1. W przypadku powzięcia decyzji w przedmiocie przeprowadzenia weryfikacji Kandydata na Dostawcę, weryfikacja przeprowadzana jest poprzez analizę złożonego przez Kandydata na Dostawcę oświadczenia w ramach wypełnienia ankiety weryfikacji Dostawcy; wzór ankiety stanowi Załącznik A do Procedury;

3.2. W przypadku powzięcia przez Administratora, na podstawie oceny wypełnionej przez Kandydata na Dostawę ankiety, wątpliwości czy daje on gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, tak by przetwarzanie spełniało wymogi RODO, Administrator może:

3.2.1. żądać dodatkowych informacji od Kandydata na Dostawcę, jeżeli w jego ocenie takie dodatkowe informacje są w danym przypadku niezbędne w celu dokonania oceny Kandydata na Dostawcę;

3.2.2. podjąć decyzję o przeprowadzeniu audytu u Kandydata na Dostawcę lub zlecić podmiotowi zewnętrznemu przeprowadzenie takiego audytu, jeżeli w jego ocenie przeprowadzenie audytu w danym przypadku jest niezbędne w celu dokonania oceny Kandydata na Dostawcę.

3.3. Ostateczną decyzję w przedmiocie zawarcia Umowy i Umowy Powierzenia z Kandydatem na Dostawcę podejmuje Administrator, na podstawie analizy całości zgromadzonego materiału.

3.4. Po przeprowadzonej czynności weryfikacji Kandydata na Dostawcę, Administrator przechowuje wypełnioną przez Dostawę ankietę wraz z podpisanym egzemplarzem Umowy oraz egzemplarzem Umowy Powierzenia.

3.5. Administrator prowadzi wykaz zawartych przez Spółkę Umów i zawartych w związku z nimi Umów Powierzenia.

4. POSTANOWIENIA KOŃCOWE

4.1. Wszystkie czynności podejmowane na podstawie Procedury są dokumentowane w formie pisemnej lub elektronicznej (w tym e-mailowej).

4.2. Integralną częścią Procedury stanowią załączniki:

4.2.1. Załącznik A – Ankieta weryfikacji Dostawcy;

4.3. Procedura jest aktualizowana przez Administratora w zależności od potrzeb.

ZAŁĄCZNIK NR 1

ANKIETA WERYFIKACJI PODMIOTU PRZETWARZAJĄCEGO

(do stosowania przed zawarciem umowy)

Nazwa podmiotu przetwarzającego	
Data wypełnienia ankiety	

Lp.	Treść pytania	Odpowiedź	Uwagi/Komentarze
Kwestie organizacyjne			
1.	Czy podmiot przetwarzający dane osobowe (**„PPDO”**) wyznaczył Inspektora Ochrony Danych (IOD)?	Tak / Nie	
2.	Jeżeli nie został wyznaczony IOD, to prosimy o wskazanie innej osoby do kontaktu w kwestiach związanych z ochroną danych osobowych.	Osoba do kontaktu: _____	
3.	Czy PPDO wprowadził środki techniczne i organizacyjne, które spełniają wymogi RODO oraz innych aktów regulujących legalne przetwarzanie danych osobowych oraz będą chroniły prawa osób, których dane dotyczą?	Tak / Nie	
4.	Czy PPDO zamierza korzystać z dalszych procesorów w procesie przetwarzania danych osobowych, które PPDO miałby przetwarzać na zlecenie Administratora danych osobowych?	Tak / Nie	
5.	Jeżeli PPDO korzysta z dalszych procesorów, to czy są oni zlokalizowani w ramach EOG? Czy dalsi procesorzy dokonują transferów danych poza EOG (niezależnie od miejsca ich siedziby)?	Tak / Nie	
6.	Czy dalsi procesorzy stosują środki techniczne i organizacyjne spełniające wymogi RODO?	Tak / Nie	

7.	Jeżeli PPDO transferuje lub jego dalsi procesorzy transferują dane poza EOG, to na jakiej podstawie prawnej? Jaki środki PPDO wdrożył w celu zapewnienia legalności takich transferów danych? Proszę podać kraje, w których będą przetwarzane powierzone dane osobowe.	Tak/Nie	
8.	Czy PPDO posiada wyspecjalizowany zespół lub doradcę zewnętrznego monitorujących zmieniające się środowisko prawne w obszarze ochrony danych osobowych? Jak często dokonywane są takie przeglądy?	Tak/Nie	
9.	Czy PPDO prowadzi regularną (bieżącą) kontrolę nad prawidłowością i legalnością przetwarzania danych przez jego dalszych procesorów? Proszę krótko opisać, na czym takie działania polegają.	Tak/Nie	
Kwestie proceduralne			
1.	Czy PPDO prowadzi rejestr czynności dla powierzonych operacji przetwarzania danych osobowych?	Tak / Nie	
2.	Czy PPDO wdrożył procedury dotyczące zarządzania incydentami bezpieczeństwa?	Tak / Nie	
3.	Czy personel PPDO został przeszkolony z zasad przetwarzania danych osobowych zgodnych z RODO, w tym zasad bezpieczeństwa?	Tak / Nie	
4.	Czy do przetwarzania danych PPDO dopuszcza wyłącznie osoby posiadające upoważnienia?	Tak / Nie	
5.	Czy personel PPDO przetwarzający dane osobowe został zobowiązany do zachowania poufności danych?	Tak / Nie	
Kwestie bezpieczeństwa			
1.	Czy PPDO wprowadził środki zapewniające, że systemy IT używane do przetwarzania danych osobowych	Tak / Nie	

	są zgodne z RODO oraz innymi aktami regulującymi przetwarzanie danych osobowych? Proszę krótko opisać wdrożone środki.		
2.	Czy PPDO przechodzi regularne audyty z zakresu bezpieczeństwa danych? Jeśli tak, to czy może udostępnić raporty? Jak często odbywają się takie audyty?	Tak / Nie	
3.	Czy PPDO podjął środki, aby zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego? Np. regularny backup. Proszę krótko opisać takie środki.	Tak / Nie	
4.	Czy PPDO posiada aktualny certyfikat ISO 27001 lub inne równoważne, np. PCI?	Tak / Nie	
5.	Czy do przetwarzania danych w pomieszczeniach PPDO, stosuje się fizyczne zabezpieczenia przed dostępem osób nieuprawnionych? Proszę krótko opisać jakie np. system kontroli dostępu, drzwi zamykane na klucz, system alarmowy, ochrona fizyczna, monitoring wizyjny.	Tak / Nie	
6.	Czy przetwarzanie danych było już przedmiotem zewnętrznych audytów lub kontroli, np. PUODO w Państwa organizacji? Jeśli tak, proszę zwięźle opisać wyniki kontroli/ audytów. Proszę również wskazać, czy wszystkie ewentualne zobowiązania nałożone przez organy nadzorcze zostały wykonane przez PPDO	Tak / Nie	
7.	Czy PPDO lub dalsi procesorzy, z których PPDO korzysta, doświadczyli istotnych incydentów naruszenia ochrony danych osobowych lub bezpieczeństwa informacji? Jeśli tak, proszę zwięźle opisać na czym one polegały, ilu podmiotów danych dotyczyły i jakie kroki zostały podjęte przez PPDO.	Tak / Nie	

Oświadczenie:

W imieniu Przetwarzającego dane osobowe oświadczam, że powyżej przekazane informacje są zgodne z prawdą. W przypadku zmiany któregokolwiek z ww. elementów, zobowiązuje się niezwłocznie (nie później niż w terminie 7 dni od wystąpienia zdarzenia) powiadomić o tym Administratora danych osobowych.

_____

podpis