

## Załącznik nr 8

### UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH (wzór)

pomiędzy:

**Narodowym Centrum Badań i Rozwoju** z siedzibą w Warszawie (00-695 Warszawa), adres: ul. Nowogrodzka 47a, zwanym dalej **Administratorem**

a

..... z siedzibą w ..... (.-...), adres: ....., zwaną dalej **Podmiot przetwarzający**.

Mając na uwadze fakt, iż:

- 1) Strony zawarły umowę dnia ..... w przedmiocie usługi polegającej na świadczenie przez Wykonawcę na rzecz Zamawiającego usług audytu bezpieczeństwa IT oraz wykonywanie testów penetracyjnych, na podstawie, której Podmiot przetwarzający zobowiązał się do przetwarzania danych osobowych (dalej „umowa”, „umowa główna”,

#### § 1

1. Przedmiotem przetwarzania są następujące kategorie (rodzaje) danych osobowych: - *nazwiska i imiona, miejsce pracy, adres zamieszkania lub pobytu, zawód, wykształcenie, numer telefonu, adres e-mail (służbowy i prywatny), seria i numer dowodu osobistego, nr konta bankowego, NIP, PESEL, nazwiska i imiona rodziców, miejsce i data urodzenia, - wszelkie inne dane wymagane do realizacji przepisów prawa nakładanych na pracodawcę/zleceniodawcę,*
2. Przekazywane na podstawie niniejszej umowy dane dotyczą następujących kategorii osób: *eksperti, beneficjenci, wnioskodawcy, personel projektu, pracownicy i współpracownicy NCBR*
3. Przetwarzanie danych przez Podmiot przetwarzający na podstawie niniejszej umowy odbywa się wyłącznie w celu realizacji Umowy głównej na polecenie Administratora.
4. Przetwarzanie danych osobowych w ramach niniejszej umowy odnosi się do następujących kategorii przetwarzań: *przeglądanie*
5. Umowa niniejsza jest zgodna z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (dalej, rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679, „RODO”) oraz powiązanymi z nim powszechnie obowiązującymi przepisami prawa polskiego.

6. Dane osobowe przetwarzane są w celu realizacji Umowy. Podmiot przetwarzający zobowiązuje się do przetwarzania powierzanych mu danych osobowych wyłącznie w zakresie i celu niezbędnym do realizacji obowiązków wynikających z Umowy głównej.

## § 2

### Obowiązki i odpowiedzialność Stron

1. Administrator oświadcza, że jest administratorem danych osobowych w rozumieniu artykułu 4 pkt 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679.
2. Podmiot przetwarzający oświadcza, że zapewnia:
  - a. wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniło wymogi RODO i chroniło prawa osób, których dane dotyczą,
  - b. dysponuje odpowiednimi środkami technicznymi i organizacyjnymi dla zapewnienia spełnienia wymogów oraz zapewnienia ochrony praw osób, których dotyczą dane osobowe, przekazywane na podstawie niniejszej umowy, zgodnie z właściwymi przepisami krajowymi, a także przyjętą przez Podmiot przetwarzający dokumentacją ochrony danych.
3. W celu prawidłowej realizacji zawartej przez Strony Umowy głównej, Administrator powierza Podmiotowi przetwarzającemu przetwarzanie danych osobowych w odniesieniu do rodzajów danych oraz kategorii osób, o których mowa w § 1 niniejszej umowy.

## § 3

1. Podmiot przetwarzający zobowiązuje się niniejszym:
  - a) przetwarzać dane osobowe zgodnie z obowiązującymi przepisami prawa oraz zasadami ochrony określonymi w niniejszej umowie;
  - b) przetwarzać dane osobowe wyłącznie na udokumentowane polecenie Administratora – co dotyczy także przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający; w takim wypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający zobowiązany jest poinformować Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielenia takiej informacji z uwagi na ważny interes publiczny;
  - c) niezwłocznie informować Administratora, jeżeli zdaniem Podmiotu przetwarzającego, wydane mu polecenie stanowi naruszenie przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 lub innych przepisów Unii Europejskiej lub przepisów krajowych o ochronie danych osobowych.

- d) dopuścić do przetwarzania danych wyłącznie osoby posiadające upoważnienie nadane przez Podmiot przetwarzający oraz zapewnić, aby osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania nieograniczonej w czasie tajemnicy, a także prowadzić ewidencję osób upoważnionych do przetwarzania danych;
- e) niezwłocznie informować Administratora danych o obowiązku prawnym udostępnienia danych osobowych, chyba że powszechnie obowiązujące przepisy zabraniają udzielenia takiej informacji z uwagi na ważny interes publiczny;
- f) podejmować wszelkie środki techniczne i organizacyjne wymagane na mocy Artykułu 32 rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679, aby zapewnić stopień bezpieczeństwa przetwarzania danych odpowiadający ryzyku naruszenia praw lub wolności osób, których dane dotyczą, w szczególności:
- pseudonimizację i/lub szyfrowanie danych osobowych,
  - zdolność do ciągłego zapewnienia poufności, integralności, dostępności systemów i usług przetwarzania danych,
  - zdolność do szybkiego przywrócenia danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
  - regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania;
- g) przestrzegać warunków korzystania z usług innego Podmiotu przetwarzającego, o których mowa w Artykule 28 ust. 2 i 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, z zastrzeżeniem § 4 ust. 1 poniżej;
- h) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomagać Administratorowi wywiązać się z obowiązków określonych w Artykułach 32 – 36 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679;
- i) niezwłocznie informować Administratora o tym, że osoba której dane dotyczą, skierowała do Podmiotu przetwarzającego korespondencję zawierającą żądanie w zakresie wykonania praw, o których mowa w rozdziale III RODO, jak również udostępniać treść tej korespondencji;
- j) udostępniać Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w Artykule 28 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 oraz umożliwiać Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji i przyczyniania się do nich;

#### § 4

1. Strony zgodnie postanawiają, że powierzenie przetwarzania danych osobowych przez Podmiot przetwarzający podmiotowi trzeciemu (dalszemu przetwarzającemu) jest

dopuszczalne wyłącznie po uzyskaniu pisemnej zgody Administratora w odniesieniu do konkretnego dalszego przetwarzającego, której wzór stanowi załącznik nr 1 do umowy.

2. W przypadku opisanym w ust. 1 Podmiot przetwarzający zobligowany będzie do umownego zobowiązania w formie pisemnej, każdego z dalszych przetwarzających do przestrzegania takich samych obowiązków i zasad, jakie dotyczą Podmiotu przetwarzającego względem Administratora na podstawie niniejszej umowy oraz przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, a także innych odnośnych przepisów dotyczących ochrony danych osobowych.
3. Podmiot przetwarzający w razie skorzystania z usług dalszego przetwarzającego zobowiązuje się nadto zapewnić, by przetwarzanie danych przez ten podmiot odbywało się wyłącznie w celu i w zakresie opisanym w niniejszej umowie.

## § 5

1. Podmiot przetwarzający zobowiązuje się do prowadzenia rejestru kategorii czynności przetwarzania, na zasadach, o których mowa w Artykule 30 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, który zawierać będzie informacje określone w pkt a – d Artykułu 30 ust. 2 rozporządzenia.
2. Podmiot przetwarzający w przypadkach, o których mowa w Artykule 37 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 zobligowany będzie do wyznaczenia inspektora ochrony danych. O fakcie wyznaczenia inspektora ochrony danych Podmiot przetwarzający powiadomi Administratora, wskazując dane kontaktowe inspektora.
3. Podmiot przetwarzający zobowiązuje się do udzielania Administratorowi na każde żądanie informacji na temat przetwarzania powierzonych danych osobowych, a w szczególności do niezwłocznego informowania o każdym przypadku naruszenia w zakresie ochrony danych osobowych.
4. Podmiot przetwarzający zobowiązany jest do wdrożenia i stosowania procedur służących wykrywaniu naruszeń ochrony danych osobowych oraz wdrażania właściwych środków naprawczych. Podmiot przetwarzający zobowiązany jest do udostępnienia procedur, o których mowa w zdaniu poprzedzającym, na żądanie Administratora. Podmiot przetwarzający zobowiązany jest do udzielenia odpowiedzi w terminie 3 dni od przesłania przez Administratora żądania, w tym zakresie.
5. Po stwierdzeniu naruszenia ochrony danych osobowych Podmiot przetwarzający bez zbędnej zwłoki, jednak nie później niż 24 godziny od powzięcia wiadomości o naruszeniu, zgłasza ten fakt Administratorowi wskazując w zgłoszeniu:
  - opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości kategorie oraz przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
  - imię i nazwisko oraz dane kontaktowe inspektora ochrony danych, lub oznaczenie innego punktu kontaktowego, od którego można pozyskać informacje,

- opis możliwych konsekwencji naruszenia ochrony danych osobowych,
  - opis środków zastosowanych lub proponowanych przez podmiot przetwarzający w celu zapobieżenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środków w celu zminimalizowania jego ewentualnych negatywnych skutków.
6. Zgłoszenie naruszenia ochrony danych osobowych następuje na adres mailowy: [inspektorochronydanychosobowych@ncbr.gov.pl](mailto:inspektorochronydanychosobowych@ncbr.gov.pl).
  7. Jeżeli informacji, o których mowa w ust. 5 powyżej nie da się ustalić w tym samym czasie Podmiot przetwarzający ma obowiązek ich udzielać sukcesywnie bez zbędnej zwłoki.
  8. Do czasu przekazania Podmiotowi przetwarzającemu instrukcji postępowania w związku z naruszeniem ochrony danych osobowych, Podmiot przetwarzający podejmuje bez zbędnej zwłoki wszelkie działania mające na celu ograniczenie i naprawienie negatywnych skutków naruszenia.
  9. Podmiot przetwarzający dokumentuje wszelkie naruszenia ochrony danych osobowych powierzonych mu przez Administratora, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze, jak również udostępnia tą dokumentację na żądanie Administratora.
  10. Podmiot przetwarzający ponosi odpowiedzialność za działania swoich pracowników i innych osób przy pomocy, których przetwarza powierzone dane osobowe, jak za własne działania i zaniechanie.
  11. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem danych osobowych w sposób naruszający przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, jeśli nie dopełnił obowiązków nałożonych na niego przez RODO lub gdy działał poza zgodnymi z prawem instrukcjami Administratora danych lub wbrew tym instrukcjom.
  12. Podmiot przetwarzający ma obowiązek współdziałać z Administratorem danych na jego żądanie w zakresie ustalenia przyczyn szkody wyrządzonej osobie, których dane dotyczą, jak również zapewnia, że obowiązek ten będzie wypełniać bezpośrednio dalszy przetwarzający w stosunku do Administratora danych.
  13. W razie stwierdzenia przez Administratora istnienia po stronie Podmiotu przetwarzającego uchybień w zakresie realizacji niniejszej umowy prowadzących do naruszenia bezpieczeństwa powierzonych do przetwarzania danych osobowych, Administrator uprawniony będzie do:
    - a) żądania niezwłocznego usunięcia uchybień;
    - b) rozwiązania niniejszej umowy oraz Umowy głównej bez zachowania okresu wypowiedzenia.
  14. W przypadku, gdy Administrator zapłaci odszkodowanie za całą wyrządzoną szkodę spowodowaną przetwarzaniem, ma prawo żądania od Podmiotu przetwarzającego zwrotu części odszkodowania odpowiadającej części szkody, za którą ponosi on odpowiedzialność.

15. Każda ze stron odpowiada za szkody wyrządzone drugiej stronie oraz osobom trzecim w związku z powierzeniem przetwarzania danych, zgodnie z przepisami kodeksu cywilnego, z zastrzeżeniem postanowień rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, wskazanych powyżej.

## § 6

### **Prawo do przeprowadzenia kontroli zgodności przetwarzania danych osobowych**

1. Strony zgodnie postanawiają, że Administrator uprawniony będzie do dokonywania kontroli prawidłowości warunków przetwarzania powierzonych na podstawie niniejszej umowy danych osobowych przez Podmiot przetwarzający, a Podmiot przetwarzający zobligowany będzie do współdziałania z Administratorem w celu realizacji powyższego zobowiązania w możliwie szerokim zakresie, tj. w szczególności udostępni administratorowi wszelkie informacje niezbędne do wykazania spełnienia przyjętych obowiązków oraz umożliwi Administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji.
2. Termin przeprowadzenia kontroli, o której mowa w ust. 1 zostanie ustalony z Podmiotem przetwarzającym, jednak kontrola nie może odbyć się później niż 5 dni roboczych od przekazania Podmiotowi przetwarzającemu
3. Podmiot przetwarzający na każdy pisemny wniosek Administratora danych zobowiązany jest do udzielenia pisemnej informacji dotyczącej przetwarzania powierzonych mu danych osobowych, w terminie 5 dni roboczych od dnia otrzymania wniosku.
4. Po przeprowadzonym audycie przedstawiciel Administratora danych lub upoważniony przez Administratora przedstawiciel audytora, sporządza protokół pokontrolny, który podpisują przedstawiciele obu Stron. Podmiot przetwarzający zobowiązuje się w terminie uzgodnionym z Administratorem, dostosować do zaleceń pokontrolnych zawartych w protokole, mających na celu usunięcie uchybień i poprawę bezpieczeństwa przetwarzania danych osobowych.
5. Administrator ma prawo żądania od Podmiotu przetwarzającego składania pisemnych wyjaśnień dotyczących realizacji niniejszej umowy.
6. Podmiot przetwarzający zobowiązany jest zapewnić w umowie z dalszym przetwarzającym, możliwość przeprowadzenia przez Podmiot przetwarzający audytu zgodności przetwarzania danych osobowych na zasadach określonych w niniejszej umowie.
7. Koszty przeprowadzenia audytu ponosi podmiot, który zlecił przeprowadzenia audytu, bez prawa do żądania zwrotu takich kosztów ani zapłaty dodatkowego wynagrodzenia.

## § 7

### **Wsparcie administratora danych w realizacji praw określonych w rozdziale III RODO**

1. Zgodnie z art. 28 ust. 3 pkt e rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, biorąc pod uwagę charakter przetwarzania, podmiot przetwarzający w miarę możliwości pomaga Administratorowi danych poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO.
2. Podmiot przetwarzający zobowiązany jest do wsparcia Administratora danych w zakresie realizacji następujących praw podmiotów danych:
  - a. Obowiązku informacyjnego, o którym mowa w art. 13 i 14 RODO,
  - b. Prawa dostępu do danych osobowych,
  - c. Prawa do sprostowania danych osobowych,
  - d. Prawo do usunięcia danych osobowych,
  - e. Prawo do ograniczenia przetwarzania,
  - f. Obowiązku informowania o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania,
  - g. Prawa do przenoszenia danych osobowych,
  - h. Prawo do sprzeciwu,
  - i. Kwestii związanych z prawem do niepodlegania zautomatyzowanemu przetwarzaniu danych osobowych, w tym profilowaniu.
3. W przypadku otrzymania żądania od Administratora danych w zakresie uzyskania wsparcia w związku z realizacją praw wymienionych w ust. 9 Podmiot przetwarzający w terminie 5 dni od otrzymania żądania poinformuje Administratora danych o wykonaniu żądania.
4. Jeżeli podmiot przetwarzający nie jest w stanie zrealizować żądania, o którym mowa w ust. 10, jest on zobowiązany do przygotowania i przekazania wyjaśnień opisujących przyczyny, dla których nie zrealizował żądania Administratora.

## § 8

### Czas trwania umowy

1. Powierzenie przetwarzania trwa przez czas obowiązywania umowy głównej.
2. Po zakończeniu świadczenia usług związanych z przetwarzaniem Podmiot przetwarzający ma obowiązek usunąć lub zwrócić Administratorowi – w zależności od decyzji Administratora- wszelkie dane osobowe, które zostały mu powierzone, jak również usunąć ich istniejące kopie, chyba że przepisy prawa powszechnego nakazują przechowywanie tych danych.

## § 9

## Postanowienia końcowe

1. Umowa została sporządzona w dwóch egzemplarzach, po jednym dla każdej ze stron.
2. W sprawach nieuregulowanych w niniejszej umowie zastosowanie mają odpowiednio przepisy prawa kodeksu cywilnego, rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, oraz innych obowiązujących przepisów z zakresu ochrony danych osobowych.
3. Podmiot przetwarzający nie może przenieść praw i obowiązków wynikających z niniejszej umowy bez pisemnej zgody Administratora danych.
4. Podmiot przetwarzający oświadcza, że znane są mu sankcje przewidziane za naruszenie obowiązków w zakresie ochrony danych osobowych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679. Jeżeli w wyniku naruszenia przez Podmiot przetwarzający przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 oraz niniejszej umowy Administrator zobligowany będzie do zapłaty kary pieniężnej lub odszkodowania, Podmiot przetwarzający zobowiązuje się zwrócić Administratorowi wszelkie poniesione z tego tytułu koszty i wydatki.
5. Zmiana niniejszej umowy nastąpić może wyłącznie w formie pisemnej pod rygorem nieważności.

### Załącznik nr 1

#### **Pisemna zgoda administratora danych na korzystanie przez podmiot przetwarzający z usług dalszych przetwarzających**

Działając w imieniu administratora danych, zgodnie z § 4 ust. 1 umowy, niniejszym wyrażam zgodę na korzystanie przez podmiot przetwarzający z usług dalszych przetwarzających na podstawie niniejszej umowy.

Oświadczam, że podmiot przetwarzający przedstawił mi listę podprocesów, z których usług korzysta. Lista stanowi załącznik do niniejszej umowy.

W imieniu administratora danych

.....  
podpis, pieczęć, data