**Załącznik nr 5 do Regulaminu rekrutacji i uczestnictwa w projekcie**

**Procedura weryfikacji wiarygodności danych przekazanych w formie elektronicznej**

**§ 1.**

**Cel i przedmiot procedury**

1. Procedura służy weryfikacji wiarygodności danych kandydatów i kandydatki oraz uczestników i uczestniczki projektu przekazanych w formie elektronicznej z uwzględnieniem konieczności:
2. przestrzegania zasad bezpieczeństwa przetwarzania danych osobowych zgodnie z RODO;
3. zapewnienia uprawnionym organom wglądu w przetwarzane dane oraz weryfikację prawdziwości zebranych danych (rozdział 8.2 pkt 8 lit. a, b, c wytycznych)
4. Procedura obejmuje proces weryfikacji wiarygodności danych przekazanych zdalnie przez kandydatów i kandydatki rekrutowanych do udziału w szkoleniach realizowanych w projekcie.
5. Procedura określa sposób przekazywania, wypełnienia, opatrywania datą, podpisywania i przechowywania dokumentów rekrutacyjnych i dokumentacji poszkoleniowej.
6. Prowadzący rekrutację nie dopuszcza potwierdzania spełnienia kryteriów kwalifikowalności uprawniających do udziału   
   w projekcie oraz złożenia oświadczenia o przyjęciu do wiadomości informacji z art. 13 i 14 RODO w formie telefonicznej.

**§ 2.**

**Bezpieczeństwo przetwarzania danych osobowych**

1. W celu zapewnienia przestrzegania zasad bezpieczeństwa przetwarzania danych osobowych zgodnie z RODO Prowadzący rekrutację:
2. wyznacza pracowników odpowiedzialnych za nadzór nad bezpieczeństwem danych osobowych uprawnionych do obsługi adresu poczty elektronicznej;
3. ograniczy dostęp do wymienionego w pkt 1 adresu poczty elektronicznej do wydzielonej stacji roboczej zabezpieczonej hasłem właściwym dla każdego profilu uprawnionego użytkownika i wyposażonej w system antywirusowy.
4. Prowadzący rekrutację zabezpiecza przed utratą prowadzoną za pośrednictwem poczty elektronicznej korespondencję przychodząca wychodzącą, wykonując regularne kopie zapasowe.
5. Dokumentacja w postaci elektronicznej (listy uczestników i uczestniczek szkoleń, informacje o specjalnych potrzebach) przekazywana przez Prowadzącego rekrutację wykonawcy odpowiedzialnemu za organizacje szkoleń jest przechowywana na właściwych do tego celu zasobach sieciowych wykonawcy, do których dostęp posiadają jedynie osoby wyznaczone przez wykonawcę. Dostęp do zasobów sieciowych zabezpieczony jest indywidualnym loginem i hasłem dla każdego upoważnionego użytkownika. Zasoby sieciowe zabezpieczone są przed utratą danych poprzez wykonywanie ich kopii bezpieczeństwa.
6. Dostęp do danych osobowych uczestników i uczestniczek mają:
7. uczestnik lub uczestniczka na podstawie 15 RODO;
8. imiennie upoważnieni pracownicy wykonawcy lub osoby, którymi wykonawca się posługuje wykonując umowę na organizację szkoleń na podstawie umowy powierzenia przetwarzania danych osobowych;
9. imiennie upoważnieni pracownicy Prowadzącego rekrutację zaangażowani w realizacje projektu.
10. Osoby, o których mowa w ust. 4 pkt 2 w ramach przetwarzania danych osobowych, w tym danych uczestników projektu są   
    w szczególności zobowiązani do:
11. przetwarzania danych osobowych zgodnie z przepisami w szczególności RODO i dokumentami wewnętrznymi obowiązującymi u wykonawcy, w tym polityką ochrony danych, oraz zgodnie z celem, dla którego te dane zostały zebrane;
12. zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczania, również po ustaniu zatrudnienia lub innego zobowiązania wynikającego z zawartych umów;
13. przetwarzania danych osobowych w wyznaczonych pomieszczeniach służbowych lub wyznaczonych ich częściach;
14. bezwzględnego przestrzegania zasad bezpieczeństwa przetwarzania informacji w systemie teleinformatycznym;
15. zabezpieczania danych osobowych oraz dokumentów zawierających dane osobowe przed dostępem osób nieupoważnionych, a w szczególności przed kradzieżą, uszkodzeniem i zaginięciem;
16. niszczenia w niszczarkach wszystkich zbędnych dokumentów zawierających dane osobowe lub w inny sposób uniemożliwiający ich odczytanie lub odtworzenie;
17. nieudzielania innym podmiotom informacji o przetwarzanych danych osobowych, chyba że obowiązek taki wynika wprost z przepisów prawa i tylko w sytuacji, gdy przesłanki określone w tych przepisach zostały spełnione;
18. zachowania szczególnej ostrożności przy wysyłaniu korespondencji tradycyjnej i elektronicznej;
19. szyfrowania korespondencji elektronicznej zawierającej dane osobowe wysyłanej za pośrednictwem poczty elektronicznej;
20. zachowania szczególnej ostrożności podczas transportu urządzeń przenośnych zawierających dane osobowe (laptopy, nośniki danych USB, dyski zewnętrzne);
21. świadczenia pracy jedynie przy użyciu dokumentów niezbędnych do wykonania obowiązków pracowniczych;
22. przechowywania dokumentów w czasie nie dłuższym niż czas niezbędny do zrealizowania zadań, do których wykonania dokumenty są przeznaczone;
23. nietworzenia kopii dokumentów innych niż niezbędne do realizacji powierzonych obowiązków.
24. Wykonawca stosuje środki techniczne i organizacyjne niezbędne dla zapewnienia przestrzegania zasad bezpieczeństwa przetwarzania danych osobowych zgodnie z RODO w postaci:

zabezpiecza urządzenia mobilne przed dostępem osób nieuprawnionych

wykonuje regularne kopie zapasowe i przechowuje je w fizycznie odrębnych lokalizacjach

stosuje środki zapewniające zdolność do szybkiego przywrócenia dostępności danych osobowych dostępu do nich w razie incydentu fizycznego, technicznego lub awarii

1. środków ochrony fizycznej danych osobowych obejmujących:
2. całodobową ochronę fizyczną,
3. stosowanie kontroli dostępu (SKD) - środków kontroli dostępu upoważnionego personelu do stref, w których przetwarzane są dane osobowe,
4. system monitoringu wizyjnego
5. zakaz pozostawiania interesantów i gości bez nadzoru w siedzibie Prowadzącego rekrutację,
6. niszczenie za pomocą niszczarek dokumentów papierowych, zewnętrznych nośników pamięci oraz płyt (CD, DVD) zawierające dane osobowe po upływie okresu ich przechowywania,
7. staranne zamykanie okien, drzwi, wyłączanie odbiorników prądu, przed ostatecznym opuszczeniem pomieszczenia,
8. stosowanie zasad czystego biurka, czystego ekranu, czystego druku, czystej tablicy i czystego kosza,
9. środków technicznych obejmujących:
10. system IDS/IPS chroniący dostęp do sieci komputerowej wykonawcy,
11. stosowanie zapór sieciowych chroniących zasoby wykonawcy przed zagrożeniami pochodzącymi z sieci publicznej,
12. system antywirusowy zabezpieczający wewnętrzne systemy wykonawcy przed złośliwym oprogramowaniem,
13. uwierzytelnianie użytkowników za pomocą identyfikatora i hasła,
14. środki ochrony kryptograficznej (szyfrowanie),
15. stosowanie mechanizmów gwarantujących regularne testowanie, mierzenie i ocenianie środków technicznych   
    i organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych;
16. środków ochrony w ramach narzędzi programowych i baz danych obejmujących:
17. zapewnienie rozliczalność operacji wykonywanych w systemie przez użytkowników na podstawie przyznanych im identyfikatorów,
18. stosowanie mechanizmu wymuszającego okresową zmianę hasła,
19. wygaszacze ekranu na stacjach roboczych;
20. środków ochrony w ramach systemu operacyjnego obejmujących:
21. scentralizowane uwierzytelnianie użytkowników domenowych na podstawie identyfikatorów i haseł,
22. stosowanie mechanizmu wymuszającego okresową zmianę hasła domenowego;
23. środków organizacyjnych obejmujących:
24. prowadzenie dokumentacji przetwarzania danych osobowych, w tym politykę ochrony danych osobowych, rejestr kategorii czynności przetwarzania,
25. zapoznanie każdej osoby zaangażowany w przetwarzanie danych osobowych przed podjęciem czynności związanych przetwarzaniem danych osobowych z obowiązującymi przepisami prawa,
26. zapewnienie bieżącego doskonalenie wiedzy osób zaangażowanych w przetwarzanie danych osobowych przez cykliczne szkolenia,
27. Pracownicy Prowadzącego rekrutację w ramach przetwarzania danych osobowych, w tym danych kandydatów i kandydatek oraz uczestników i uczestniczek projektu są w szczególności zobowiązani do:
28. przetwarzania danych osobowych zgodnie z przepisami, w szczególności RODO oraz dokumentami wewnętrznymi obowiązującymi w Narodowym Centrum Krwi, w tym Polityką Ochrony Danych Osobowych stanowiącą załącznik do zarządzenia nr 131 Dyrektora Narodowego Centrum Krwi z dnia 1 lipca 2019 r., oraz zgodnie z celem, dla którego te dane zostały zebrane;
29. przetwarzania danych osobowych w ramach udzielonych imiennych upoważnień nadawanych po przeprowadzeniu szkolenia;
30. zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczania, również po ustaniu zatrudnienia lub innego zobowiązania wynikającego z zawartych umów;
31. przetwarzania danych osobowych w odpowiednio zabezpieczonych pomieszczeniach służbowych lub wyznaczonych ich częściach;
32. bezwzględnego przestrzegania zasad bezpieczeństwa przetwarzania informacji w systemie teleinformatycznym;
33. zabezpieczania danych osobowych oraz dokumentów zawierających dane osobowe przed dostępem osób nieupoważnionych, a w szczególności przed kradzieżą, uszkodzeniem i zaginięciem;
34. niszczenia w niszczarkach wszystkich zbędnych dokumentów zawierających dane osobowe lub w inny sposób uniemożliwiający ich odczytanie lub odtworzenie;
35. nieudzielania innym podmiotom informacji o przetwarzanych danych osobowych, chyba że obowiązek taki wynika wprost z przepisów prawa i tylko w sytuacji, gdy warunki określone w tych przepisach zostały spełnione;
36. zachowania szczególnej ostrożności przy wysyłaniu korespondencji tradycyjnej i elektronicznej;
37. szyfrowania korespondencji elektronicznej wysyłanej za pośrednictwem poczty elektronicznej;
38. zachowania szczególnej ostrożności podczas transportu urządzeń przenośnych zawierających dane osobowe (laptopy, nośniki danych USB, dyski zewnętrzne);
39. świadczenia pracy jedynie przy użyciu dokumentów niezbędnych do wykonania obowiązków pracowniczych;
40. przechowywania dokumentów w czasie nie dłuższym niż czas niezbędny do zrealizowania zadań, do których wykonania dokumenty są przeznaczone;
41. nietworzenia kopii dokumentów innych niż niezbędne do realizacji powierzonych obowiązków.
42. W celu zapewnienia przestrzegania zasad bezpieczeństwa przetwarzania danych osobowych zgodnie z RODO Prowadzący rekrutację stosuje środki techniczne i organizacyjne w postaci:
43. środków ochrony fizycznej danych osobowych obejmujących:
44. ustalenie zasad udostępniania kluczy do pomieszczeń i szaf - wydawanie i zdawanie kluczy do pomieszczeń   
    z wykorzystaniem elektronicznego depozytora kluczy zapewniającego ewidencjonowanie wykonanych czynności,
45. lokalizację miejsc przetwarzania danych osobowych w pomieszczeniach o ograniczonym i kontrolowanym dostępie,
46. przechowywanie szczególnych kategorii danych osobowych, nośników wymiennych i nośników kopii zapasowych w zabezpieczonych szafach,
47. system kontroli dostępu (SKD) – drzwi wejściowe otwierane przez właściwego pracownika po zweryfikowania tożsamości osób wchodzących,
48. system monitoringu wizyjnego,
49. zakaz pozostawiania interesantów i gości bez nadzoru w siedzibie Prowadzącego rekrutację,
50. niszczenieza pomocą niszczarek dokumentów papierowych, zewnętrznych nośników pamięci oraz płyt (CD, DVD) zawierające dane osobowe po upływie okresu ich przechowywania,
51. staranne zamykanie okien, drzwi (w określonych przypadkach plombowanie) i krat, wyłączanie odbiorników prądu   
    i włączanie alarmu, przed ostatecznym opuszczeniem pomieszczenia,
52. stosowanie zasad czystego biurka, czystego ekranu, czystego druku, czystej tablicy i czystego kosza,
53. zakaz kierowania monitorów w kierunku okien i drzwi,
54. przebywanie w siedzibie Prowadzącego rekrutację po godzinach pracy tylko za zgodą przełożonego,
55. niezwłoczne powiadamianie bezpośredniego przełożonego o każdym przypadku utraty klucza do pokoju służbowego oraz o każdej innej sytuacji, gdy mogło nastąpić naruszenie zabezpieczeń pomieszczenia (włamanie/kradzież),
56. każdorazowe zamykanie pomieszczeń na czas nieobecności pracujących w nich osób;
57. środków technicznych obejmujących:
58. scentralizowaną kontrolę dostępu do systemu informatycznego,
59. system wykrywania i blokowania włamań (IPS) chroniący dostęp do sieci komputerowej Prowadzącego rekrutację,
60. zapory sieciowe chroniące zasoby Prowadzącego rekrutację przed zagrożeniami pochodzącymi z sieci publicznej,
61. system antywirusowy,
62. system automatycznej aktualizacji komputerów na których przetwarzane są dane osobowe,
63. system ochrony poczty e-mail,
64. segmentację sieci (WAN, DMZ, LAN, WiFI),
65. stosowanie rozwiązań typu VPN,
66. ochronę użytkowników przed niebezpiecznymi witrynami internetowymi (WEB filtering),
67. stosowanie ochrony przed nieznanymi zagrożeniami (sandboxing),
68. zabezpieczenia serwerów (zasilacze, wentylatory, dyski w konfiguracji RAID, klimatyzacja, monitorowanie temperatury z automatycznym powiadamianiem),
69. zarządzanie urządzeniami z wydzielonych podsieci, do których nieuprawnieni pracownicy Prowadzącego rekrutację nie mają dostępu,
70. urządzenia UPS i wydzielona sieć elektroenergetyczna chronią system służący do przetwarzania danych osobowych przed skutkami awarii zasilania,
71. system antywirusowy zabezpieczający wewnętrzne systemy przed złośliwym oprogramowaniem,
72. uwierzytelnienie użytkowników systemów informatycznych za pomocą identyfikatora i hasła oraz stosowanie uwierzytelnienia dwuetapowego (2FA),
73. środki ochrony kryptograficznej (szyfrowanie),
74. stosowanie mechanizmów gwarantujących regularne testowanie, mierzenie i ocenianie środków technicznych   
    i organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych;
75. środków ochrony w ramach narzędzi programowych i baz danych obejmujących:
76. zapewnienie rozliczalności operacji wykonywanych w systemie przez użytkowników na podstawie przyznanych im identyfikatorów;
77. stosowanie mechanizmu wymuszającego okresową zmianę hasła,
78. stosowanie wygaszaczy ekranu na stacjach roboczych,
79. stosowanie mechanizmu automatycznej blokady dostępu systemu operacyjnego w przypadku dłuższej nieaktywności pracy użytkownika;
80. środków ochrony w ramach systemu operacyjnego obejmujących:
81. scentralizowane uwierzytelnianie użytkowników domenowych na podstawie identyfikatorów i haseł,
82. stosowanie mechanizmu wymuszającego okresową zmianę hasła domenowego;
83. kontrolę uprawnień użytkowników przez stosowanie grup użytkowników o określonych uprawnieniach;
84. środków organizacyjnych obejmujących:
85. podział kompetencji między podmioty pełniące funkcje w systemie ochrony danych osobowych (administrator danych, inspektor ochrony danych, administrator systemów informatycznych, osoby upoważnione doi przetwarzania danych osobowych),
86. prowadzenie dokumentacji przetwarzania danych osobowych – rejestru czynności przetwarzania danych osobowych, rejestru kategorii czynności przetwarzania, rejestru naruszeń ochrony danych osobowych, ewidencji osób upoważnionych do przetwarzania danych osobowych,
87. przeprowadzanie analizy ryzyka dla praw i wolności osób fizycznych związanych z przetwarzaniem ich danych osobowych i oceny skutków dla ochrony danych j
88. dopuszczenie do przetwarzania danych osobowych wyłącznie osób imiennie upoważnionych,
89. zapoznanie osób upoważnionych z zasadami przetwarzania danych osobowych i obsługą systemu informatycznego do ich przetwarzania i pozyskanie od tych osób oświadczeń o zapoznaniu z przepisami określającymi zasady postępowania przy przetwarzaniu danych osobowych,
90. prowadzenie przez inspektora ochrony danych audytów zgodności przetwarzania danych osobowych z przepisami   
    o ochronie danych osobowych na podstawie planu audytów,
91. ubezpieczenie sprzętu przed kradzieżą lub zniszczeniem.
92. Wskazane w ust. 8 środki techniczne i organizacyjne zostały wprowadzone na podstawie zarządzeń Dyrektora Narodowego Centrum Krwi, w szczególności:
93. zarządzenie nr 34 Dyrektora Narodowego Centrum Krwi z dnia 14 września 2011 r. w sprawie wprowadzenia regulaminu użytkowania sieci teleinformatycznej Narodowego Centrum Krwi;
94. zarządzenie nr 51 Dyrektora Narodowego Centrum Krwi z dnia 15 lutego 2013 r. w sprawie polityki bezpieczeństwa   
    i zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Narodowym Centrum Krwi ;
95. zarządzenie nr 131 Dyrektora Narodowego Centrum Krwi z dnia 1 lipca 2019 r. w sprawie wprowadzenia Polityki ochrony danych osobowych w Narodowym Centrum Krwi;
96. zarządzenie nr 25/2021 Dyrektora Narodowego Centrum Krwi z dnia 27 grudnia 2021 r. w sprawie wprowadzenia Regulaminu określającego wewnętrzną procedurę zgłaszania naruszeń prawa obowiązującą w Narodowym Centrum Krwi oraz powołania Komisji do spraw badania naruszeń prawa;
97. zarządzenie nr 12/2022 Dyrektora Narodowego Centrum Krwi z dnia 14 września 2022 r. w sprawie wprowadzenia Karty Audytu Wewnętrznego w Narodowym Centrum Krwi;
98. zarządzenie nr 6/2022 Dyrektora Narodowego Centrum Krwi z dnia 31 stycznia 2022 r. w sprawie wprowadzenia do stosowania polityki zarządzania ryzykiem w Narodowym Centrum Krwi;
99. zarządzenie nr 18 Dyrektora Narodowego Centrum Krwi z dnia 29 grudnia 2022 r. w sprawie wprowadzenia instrukcji kancelaryjnej, jednolitego rzeczowego wykazu akt oraz instrukcji w sprawie organizacji i zakresu działania archiwum zakładowego;
100. zarządzenie nr 3/2023 Dyrektora Narodowego Centrum Krwi z dnia 7 kwietnia 2023 r. w sprawie regulaminu pracy zdalnej w Narodowym Centrum Krwi.

**§ 3.**

**Wgląd w dane osobowe i weryfikacja prawdziwości danych osobowych**

1. Dokumenty rekrutacyjne przesłane w formie papierowej są przechowywane w siedzibie Prowadzącego rekrutację   
   w segregatorach w szafach zamykanych na klucz, do których dostęp mają jedynie osoby zaangażowane w realizację projektu oraz zgodnie z zarządzeniami, o których mowa w §2 ust. 9 pkt 3 i 7.
2. Dokumenty rekrutacyjne przesłane w postaci elektronicznej są przechowywane na serwerach Prowadzącego rekrutację   
   w folderze, do którego dostęp mają jedynie osoby zaangażowane w realizację projektu.
3. W celu weryfikacji prawdziwości zebranych danych na żądanie uprawnionych organów kontroli uczestnicy lub uczestniczki projektu potwierdzają prawdziwość przekazanych danych na dalszym etapie realizacji projektu:
4. telefonicznie, udzielając niezbędnych wyjaśnień przedstawicielowi uprawnionych organów kontroli lub
5. w formie krótkiej wiadomości tekstowej wiadomości (sms) wysłanej przedstawicielowi uprawnionych organów kontroli lub
6. wiadomości e-mailowej wysłanej na skrzynkę e-mailową przedstawiciela uprawnionych organów kontroli.