

„ZATWIERDZAM”
DYREKTOR
EKSPERCKIEGO CENTRUM SZKOLENIA
CYBERBEZPIECZEŃSTWA

pik. Mariusz KRAWCZYK
(podpis, data)

REGULAMIN

Projektu Akademia_CYBER.MIL w roku akademickim 2026/2027

§ 1. Postanowienia ogólne dotyczące realizacji Projektu

1. Niniejszy Regulamin (dalej: Regulamin) określa warunki i zasady realizacji Projektu Akademia_CYBER.MIL.
2. Podstawą wdrożenia Projektu Akademia_CYBER.MIL (dalej: Projekt) jest uchwała nr 92 Rady Ministrów z dnia 10 marca 2026 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej (M.P. z 2026 r., poz. 309) oraz decyzja Nr 347/ECSC Ministra Obrony Narodowej z dnia 17 września 2026 r. w sprawie realizacji Projektu Akademia_CYBER.MIL w roku akademickim 2026/2027, dotycząca wsparcia publicznych uczelni w procesie kształcenia na kierunkach związanych z obszarem informatyki lub cyberbezpieczeństwa.
3. Organizatorem Projektu jest Ministerstwo Obrony Narodowej (dalej: MON), reprezentowane przez Eksperskie Centrum Szkolenia Cyberbezpieczeństwa (dalej zamiennie jako: ECSC lub Organizatorzy).
4. Nadzór nad realizacją Projektu sprawuje Dyrektor Departamentu Cyberbezpieczeństwa MON.
5. Celem głównym Projektu jest podnoszenie poziomu kompetencji studentów w obszarze cyberbezpieczeństwa, budowanie świadomości zagrożeń w cyberprzestrzeni oraz popularyzowanie wizerunku resortu obrony narodowej (dalej: RON) jako atrakcyjnego miejsca do podjęcia pracy i służby.
6. Projekt w roku akademickim 2026/2027 skierowany jest do wszystkich publicznych uczelni prowadzących studia pierwszego lub drugiego stopnia lub jednolite studia magisterskie działających na obszarze Rzeczypospolitej Polskiej, które prowadzą kształcenie w obszarze informatyki lub cyberbezpieczeństwa. Uczelnie przystępują do Projektu poprzez zgłoszenie udziału oraz wyznaczenie koordynatora odpowiedzialnego za współpracę organizacyjną z Organizatorami, w szczególności w zakresie rekrutacji studentów, przekazywania informacji oraz organizacji udziału w poszczególnych etapach przedsięwzięcia. Uczelnie w terminie do dnia 16 października 2026 r. poprzez stronę ECSC <https://ecsc.mil.pl/> (w zakładce dedykowanej Projektowi) wypełnią deklarację chęci udziału w przedmiotowym Projekcie.
7. W ramach Projektu przewiduje się:
 - 1) przeprowadzenie szkoleń z obszaru informatyki i cyberbezpieczeństwa przez ECSC oraz wsparcie merytoryczne udzielane przez inne komórki i jednostki organizacyjne RON,

- zaangażowane w Projekt, a także organizację i przeprowadzenie stacjonarnych zawodów CTF (dla maksymalnie 16 uczelni);
- 2) promowanie Projektu na uczelniach oraz inspirowanie środowiska akademickiego do angażowania się w realizację innych projektów takich jak: „Zostań Żołnierzem Rzeczypospolitej” a także ochotniczego szkolenia wojskowego studentów i absolwentów uczelni w ramach programu Legii Akademickiej.
8. W ramach Projektu zakłada się trzy etapy:
 - a) zdalne szkolenia synchroniczne z obszaru informatyki i cyberbezpieczeństwa przeprowadzane, z wykorzystaniem platformy Microsoft Teams,
 - b) testy wiedzy po ukończonych szkoleniach na platformie e-learningowej ECSC,
 - c) ogólnopolskie stacjonarne zawody CTF.
 9. Zakłada się przeprowadzenie dla studentów uczelni biorących udział w Projekcie (osób kształcących się na studiach pierwszego lub drugiego stopnia lub jednolitych studiach magisterskich) oraz posiadających obywatelstwo polskie, w okresie od listopada 2026 r. do stycznia 2027 r., zdalnych szkoleń synchronicznych przez instruktorów i ekspertów ECSC, z wykorzystaniem platformy Microsoft Teams.
 10. Szkolenia przeprowadzone będą wg poniższego harmonogramu:
 - 1) Moduł „Cyberhigiena” (ECSC) – realizacja szkoleń w formule „live online” w okresie od 2 listopada 2026 r. do 20 listopada 2026 r.
 - 2) Moduł „Ekspozycja cyfrowa jako wektor ataku” (ECSC) – realizacja szkoleń w formule „live online” w okresie od 30 listopada 2026 r. do 18 grudnia 2026 r.
 - 3) Moduł „Dezinformacja i operacje informacyjne w cyberprzestrzeni” (ECSC) – realizacja szkoleń w formule „live online” w okresie od 4 stycznia 2027 r. do 22 stycznia 2027 r.
 11. Szczegółowe terminy szkoleń, o których mowa w pkt 10 zostaną przesłane do koordynatorów z uczelni.
 12. Każde szkolenie zakończone będzie testem wiedzy udostępnionym na platformie e-learningowej ECSC. Do zaliczenia testu wiedzy konieczne jest udzielenie 70% poprawnych odpowiedzi.
 13. Po uzyskaniu pozytywnego wyniku z testu wiedzy, po każdym szkoleniu będzie możliwość wygenerowania zaświadczenia o jego ukończeniu po wcześniejszym wypełnieniu ankiety satysfakcji na platformie e-learningowej ECSC.
 14. Zgłoszeni przez uczelnie studenci będą mieli możliwość wzięcia udziału w dowolnej liczbie szkoleń.
 15. Studenci zainteresowani wzięciem udziału w Projekcie zgłaszają się do wyznaczonego przez Rektora koordynatora z uczelni. Informację w tej sprawie posiada Biuro Karier na uczelni.
 16. W celu dostępu do platformy Microsoft Teams studenci biorący udział w Projekcie będą używać adresów e-mail z domeną uczelni.
 17. Przed terminem przeprowadzenia danego szkolenia na platformie Microsoft Teams, na wskazane przez studentów zgłoszonych do udziału w Projekcie adresy e-mail z domeną uczelni, zostaną przesłane linki z instrukcją dostępu do szkoleń, o których mowa w pkt 10.
 18. Warunkiem koniecznym do zakończenia szkolenia jest wypełnienie ankiety zamieszczonej na platformie e-learningowej ECSC, po jego zakończeniu.

§ 2. Zasady organizacji ogólnopolskich stacjonarnych zawodów Capture The Flag

1. Organizatorem ogólnopolskich stacjonarnych zawodów Capture The Flag (dalej: zawody CTF) jest Ministerstwo Obrony Narodowej, reprezentowane przez Eksperckie Centrum Szkolenia Cyberbezpieczeństwa (dalej: Organizatorzy) pod nadzorem Departamentu Cyberbezpieczeństwa MON (DC MON).
2. Zawody CTF odbędą się w dniu 5 maja 2027 r. w Centrum Konferencyjnym Wojska Polskiego (ul. Żwirki i Wigury 9/13, 02-143 Warszawa). Oficjalne rozpoczęcie zawodów CTF nastąpi o godz. 8:00.
3. W dniu zawodów należy stawić się w miejscu wskazanym w pkt 2 o godz.: 7:00, z dokumentem potwierdzającym tożsamość, w celu rejestracji i pobrania pakietu startowego (materiały promocyjne).
4. Organizatorzy zastrzegają sobie prawo do zmiany terminu zawodów CTF, jeśli taka zmiana będzie uzasadniona względami organizacyjnymi.
5. Przejazd na zawody CTF i ewentualny nocleg uczestnicy organizują we własnym zakresie.
6. Zawody CTF skierowane są do studentów uczelni zakwalifikowanych do udziału w Projekcie.
7. Do zawodów CTF zakwalifikuje się maksymalnie 16 zespołów uczelnianych wyłonionych na podstawie wyników uzyskanych w testach wiedzy po szkoleniach.
8. ECSC poinformuje uczelnie o zakwalifikowaniu do zawodów CTF.
9. Równolegle, lista uczelni zakwalifikowanych do zawodów CTF zostanie opublikowana na stronie ECSC.
10. Każda uczelnia uczestnicząca w Projekcie jest uprawniona do zgłoszenia jednego pięcioosobowego zespołu, który będzie reprezentował uczelnię w zawodach CTF.
11. Ustalenie składu zespołu biorącego udział w zawodach CTF pozostawia się w gestii władz poszczególnych uczelni z zastrzeżeniem założeń zawartych w pkt 12.
12. W skład zespołu biorącego udział w zawodach CTF mogą wchodzić studenci danej uczelni (osoby kształcące się na studiach pierwszego lub drugiego stopnia albo jednolitych studiach magisterskich) posiadający obywatelstwo polskie oraz wykazujący się szczególnymi osiągnięciami w obszarze informatyki lub cyberbezpieczeństwa.
13. Każdy zespół może wycofać się z zawodów CTF, w dowolnym czasie. Wycofanie jest równoznaczne z utratą prawa do nagród, o których mowa w pkt 44 - 45.
14. W terminie do dnia 19 kwietnia 2027 r. uczelnie prześlą na wskazany adres e-mail ECSC skład zespołów zawodów CTF wykorzystując formularz umieszczony na stronie ECSC w zakładce dedykowanej Projektowi. Formularz będzie zawierał: nazwę uczelni, imiona i nazwiska studentów, e-maile studentów z domeną uczelni, numery kontaktowe studentów oraz wskazanie lidera zespołu.
15. Weryfikacji zespołów dokona ECSC.
16. Zawody CTF będą polegały na wykonaniu jak największej ilości zadań z zakresu cyberbezpieczeństwa w wyznaczonym czasie.
17. W ramach prowadzonych zawodów CTF zespoły będą rywalizowały między sobą, gromadząc punkty w różnych konkurencjach na konto swojego zespołu.
18. Warunkiem uczestnictwa w zawodach CTF przez studentów wytypowanych do reprezentowania uczelni jest:
 - 1) ukończenie przez studenta najpóźniej w dniu rozpoczęcia zawodów 18 lat;
 - 2) posiadanie obywatelstwa polskiego;
 - 3) posiadanie pełnej zdolności do czynności prawnych;
 - 4) podpisanie Oświadczenia o zapoznaniu się z Regulaminem (wzór Oświadczenia określa Załącznik nr 1 do Regulaminu);

- 5) zachowania poufności w zakresie określonym w Regulaminie Projektu.
19. Przed przystąpieniem do udziału w zawodach CTF uczestnik powinien zapoznać się z niniejszym Regulaminem dostępnym u koordynatorów z uczelni oraz na stronie internetowej www.ecsc.mil.pl w zakładce dedykowanej Projektowi.
 20. Udział w zawodach CTF jest równoznaczny z akceptacją Regulaminu.
 21. Podczas zawodów CTF członkowie zespołów otrzymają jednorazowe kody pozwalające na założenie konta na dedykowanej platformie i udział w rozwiązywaniu zadań konkursowych.
 22. Organizatorzy zapewnią uczestnikom dostęp do sieci komputerowej.
 23. Uczestnicy zawodów CTF korzystają z własnych komputerów. Konieczne jest posiadanie w komputerze przenośnym (notebooku) karty sieciowej, Ethernet, 100/1000Mbit/s ze złączem RJ45 i ewentualnie w przypadku chęci skorzystania z dodatkowego monitora posiadania złącza HDMI. Preferowany system operacyjny komputerów to Kali Linux lub ewentualnie maszyna wirtualna z tym systemem.
 24. Organizatorzy zapewnią dostęp do platformy wymienionej w pkt 21 dla każdego członka zespołu.
 25. Momentem rozpoczęcia zawodów CTF jest oficjalne przedstawienie treści zadań podczas otwarcia zawodów. Dopiero od tego momentu możliwe jest zapoznanie się przez zespoły z treścią zadań i rozpoczęcie ich rozwiązywania.
 26. Po zapoznaniu się z tematem zadań i ogłoszeniem otwarcia zawodów CTF, każdy z uczestników otrzyma instrukcję wykonywania zadań wraz z ich punktacją. Zawody będą trwały maksymalnie 8 godzin.
 27. Organizatorzy zastrzegają sobie prawo modyfikacji zadań. Każdy zespół będzie powiadomiony o wprowadzonej modyfikacji w celu doprecyzowania lub naprawienia błędu w zadaniu poprzez platformę.
 28. Aby rozwiązać zadanie należy znaleźć ukrytą flagę - specjalny ciąg znaków udowadniający rozwiązanie zadania lub wykonać określone czynności zmierzające do udzielenia odpowiedzi na pytanie. Za zgłoszenie za pomocą platformy flagi lub odpowiedzi uczestnicy dostają punkty. Znalezienie i zgłoszenie flagi lub udzielenie odpowiedzi na pytanie jest celem każdego zadania.
 29. Organizatorzy zawodów zapewnią uczestnikom kanał komunikacyjny (np. czat) umożliwiający zgłaszanie problemów z platformą i zadaniami w czasie trwania zawodów CTF.
 30. Uczestnicy zawodów CTF zobowiązują się wykonać zadania stanowiące przedmiot zawodów samodzielnie i bez pomocy z zewnątrz.
 31. Uczestnikom zawodów CTF nie wolno, pod rygorem natychmiastowego wykluczenia z udziału w zawodach, podejmować prób uzyskania dostępu do treści zadania przed rozpoczęciem zawodów.
 32. Organizatorzy mają prawo wykluczyć zespół z zawodów CTF, w przypadku podejmowania działań łamiących postanowienia Regulaminu lub przepisów prawa powszechnie obowiązującego np.: ataki na infrastrukturę teleinformatyczną, niszczenie infrastruktury, niszczenie zadań lub utrudnianie rozwiązywania ich przez uczestników innych zespołów.
 33. Organizatorzy zawodów CTF wskażą skład trzyosobowej Komisji oceniającej zawody.
 34. Komisja oceniająca ze swego grona wybierze przewodniczącego.
 35. Komisja dokona oceny zadań realizowanych przez poszczególne zespoły, z czego sporządzi protokół, dokona wyłonienia zwycięzców oraz ogłosi wyniki zawodów CTF.
 36. Zakres wiedzy uczestników zawodów CTF nie podlega ocenie przez Komisję oceniającą.
 37. Decyzja Komisji oceniającej jest ostateczna i nie podlega odwołaniu.

38. Podczas trwania zawodów CTF, wyznaczone przez Organizatorów osoby zapewnią doraźną pomoc techniczną dla uczestników zawodów w zakresie platformy (wsparcie techniczne oraz merytoryczne, bez podpowiedzi dotyczących sposobu rozwiązywania zadań).
39. Studenci biorący udział w zawodach CTF będą mieli zapewnione bezpłatne wyżywienie podczas ich trwania.
40. Za uczestnictwo w zawodach CTF dla wszystkich uczestników przewidziane są pakiety startowe.
41. Rozstrzygnięcie ogólnopolskich stacjonarnych zawodów CTF nastąpi w dniu 5 maja 2027 r.
42. Zwycięzcy zawodów CTF zostaną powiadomieni o wynikach zawodów w formie ustnej.
43. Na zakończenie zawodów CTF nastąpi uroczyste zakończenie Projektu z wręczeniem dyplomów i nagród.
44. Zespoły, które zajmą I, II i III miejsce w zawodach CTF, otrzymają od Organizatorów bilety na Konferencję CyberEXPERT organizowaną przez ECSC w listopadzie 2027 r.
45. Zwycięzcy zawodów CTF otrzymają nagrodę specjalną w postaci pakietu przygotowanego przez Akademię Marynarki Wojennej im. Bohaterów Westerplatte z siedzibą w Gdyni (dalej: AMW) obejmującego wizytę i zwiedzanie gmachu AMW, zwiedzanie Portu Wojennego w Gdyni oraz rejs łodzią motorową po Zatoce Gdańskiej.
46. Dla wszystkich uczelni biorących udział w zawodach CTF przewiduje się pamiątkowe deski okolicznościowe.
47. Warunkiem wydania nagród jest obecność podczas ogłaszania wyników zawodów CTF. Brak obecności powoduje utratę nagrody.
48. Laureaci mają prawo do rezygnacji z przyjęcia nagrody.
49. Wydarzenia stanowiące nagrody, o których mowa w pkt 44-45, odbędą się w miejscu, czasie i na warunkach ustalonych przez Organizatorów.
50. Uczestnicy zawodów CTF są zobowiązani do zachowania w poufności informacji chronionych, o których mowa w pkt 52.
51. W celu uniknięcia jakichkolwiek wątpliwości Organizatorzy informują, że użyte w Regulaminie określenie *Informacje chronione* nie dotyczy informacji niejawnych w rozumieniu *Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (tj. Dz. U. z 2019 poz. 412 ze zm.)*.
52. Informacje chronione to treści zadań zawodów, informacje, wiedza, dane, jak również dokumenty i projekty dokumentów (także w postaci nieukończonych) udostępnione przez Organizatorów lub opracowane/przygotowane przez uczestników zawodów CTF w czasie ich trwania oraz 12 miesięcy po ich zakończeniu. To również informacje o charakterze technicznym, technologicznym (w tym dokumenty, oprogramowanie, dane), lub inne informacje uzyskane w wyniku analizy, lub przetworzenia dostarczonych informacji (w tym danych osobowych) oraz które:
 - 1) nie zostały podane do publicznej wiadomości;
 - 2) które uczestnicy zawodów CTF uzyskali i/lub które mogą stać się im znane w toku rozmów i/lub w związku z wykonywaniem przez uczestników zawodów.
53. Informacje chronione będą wykorzystywane przez uczestnika zawodów CTF wyłącznie w celu udziału w zawodach.
54. Organizatorzy informują, że zobowiązanie do zachowania w poufności Informacji chronionych obejmuje m.in.:
 - 1) zakaz rozpowszechniania, kopiowania lub dystrybucji, ujawniania, przekazywania, potwierdzania i/lub składania komentarzy dotyczących Informacji chronionych wobec osób i podmiotów trzecich i/lub nieupoważnionych osób, pośrednio bądź bezpośrednio;

- 2) obowiązek niezwłocznego poinformowania Organizatorów o fakcie utraty, ujawnienia lub powielenia Informacji chronionej i/lub niedotrzymania warunków Regulaminu.
55. Uczestnik zawodów CTF zobowiązuje się zwrócić Organizatorom wszelkie urządzenia, dokumenty (włączając ich kopie) oraz nośniki danych niezwłocznie po ich wykorzystaniu lub użyciu w związku z udziałem w zawodach CTF, oraz usunąć dane i informacje zapisane w pamięci komputera lub na innych nośnikach danych.
56. Organizatorzy zastrzegają sobie prawo odwołania zawodów CTF przed czasem bez podania przyczyny.
57. Organizatorzy zastrzegają sobie prawo do dokonania zmian w Regulaminie bez konsultacji z uczestnikami zawodów CTF.

§ 3. Ochrona danych osobowych

1. Administratorem danych osobowych uczestników biorących udział w Projekcie Akademia_CYBER.MIL w rozumieniu art. 13 *Rozporządzenia Parlamentu Europejskiego i Rady (DE) 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* jest Eksperckie Centrum Szkolenia Cyberbezpieczeństwa (dalej: ECSC) reprezentowane przez Dyrektora ECSC z siedzibą w Warszawie, przy ul. gen. S. Kaliskiego 2.
2. Klauzula informacyjna RODO stosowana przy Projekcie Akademia_CYBER.MIL w roku akademickim 2026/2027 wobec koordynatorów oraz studentów uczelni biorących w nim udział stanowi Załącznik nr 2 do Regulaminu.

OŚWIADCZENIE

uczestnika ogólnopolskich zdalnych/stacjonarnych (*należy podkreślić właściwą opcję*) zawodów
Capture The Flag

Ja (*imię i nazwisko*)

Student (*nazwa uczelni*)

na kierunku

oświadczam, iż:

1. Jestem pełnoletnia/ni i posiadam pełną zdolność do czynności prawnych.
2. Posiadam obywatelstwo polskie.
3. Zapoznałem się z Regulaminem Projektu Akademia_CYBER.MIL, akceptuję go oraz zobowiązuję się do jego przestrzegania.
4. Zobowiązuję się do zachowania poufności w zakresie określonym w Regulaminie Projektu Akademia_CYBER.MIL.

.....
(*data i podpis studenta*)

Wyrażam zgodę na dokumentowanie i utrwalanie wybranych przez Organizatorów zdarzeń w ramach ogólnopolskich stacjonarnych zawodów CTF, włącznie z rejestrowaniem dźwięku i obrazu, a w szczególności utrwalania mojego wizerunku w celu późniejszego wykorzystania tych materiałów do celów związanych z informowaniem przez Organizatorów o przebiegu zawodów i jego wyniku.

.....
(*data i podpis studenta*)

KLAUZULA INFORMACYJNA Z RODO

stosowana przy Projekcie Akademia_CYBER.MIL w roku akademickim 2026/2027

wobec koordynatorów oraz studentów uczelni biorących w nim udział

Działając na podstawie art. 14 ust. 1 i 2 RODO, informuję Panią/Pana, że:

Administratorem danych osobowych jest Eksperckie Centrum Szkolenia Cyberbezpieczeństwa – dalej ECSC – reprezentowane przez Dyrektora ECSC, z siedzibą w Warszawie, 00-908, przy ul. gen. Sylwestra Kaliskiego 2, e-mail: sekretariat.ecsc@mon.gov.pl, tel. 261-837-990.

Administrator wyznaczył Inspektora Ochrony Danych, z którym można się kontaktować poprzez pocztę elektroniczną na adres: ecsc.iod@mon.gov.pl lub telefonicznie: 261-837-990.

Pani/Pana dane osobowe – imię i nazwisko; nazwa uczelni; adres e-mail z domeną uczelni; nazwa kierunku studiów oraz rok studiów – pozyskane zostały od Pani/Pana macierzystej uczelni w związku z przystąpieniem przez Panią/Pana do projektu Projektu_Akademia_CYBER.MIL i przetwarzane będą w związku z realizacją *Decyzji Nr 347/ECSC Ministra Obrony Narodowej z dnia 17 września w sprawie realizacji Projektu_Akademia_CYBER.MIL w roku akademickim 2026/2027*, która służy do wykonania zadania realizowanego w interesie publicznym.

Podstawą prawną przetwarzania danych osobowych jest art. 6 ust. 1 lit. e RODO w związku z art. 2 pkt 1 i pkt 23 ustawy z dnia 14 grudnia 1995 r. o urzędzie Ministra Obrony Narodowej (Dz. U. z 2025 poz. 445), § 2 pkt 3a rozporządzenia Rady Ministrów z dnia 9 lipca 1996 r. w sprawie szczegółowego zakresu działania Ministra Obrony Narodowej (Dz. U. z 2026 poz. 531) oraz *decyzją Nr 347/ECSC Ministra Obrony Narodowej z dnia 17 września w sprawie realizacji Projektu_Akademia_CYBER.MIL w roku akademickim 2026/2027*.

Podstawa prawną przetwarzania danych osobowych przez ww. administratora jest także art. 10 ust. 4 ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny (Dz. U. z 2025 poz. 825) w związku z uchwałą nr 92 Rady Ministrów z dnia 10 marca 2026 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej (M.P. poz. 309).

Dane osobowe będą przekazywane podmiotom przetwarzającym dane osobowe na zlecenie administratora, a także innym podmiotom uprawnionym na podstawie przepisów prawa, w tym podmiotom współrealizującym Projekt_Akademia_CYBER.MIL.

Dane nie będą przekazywane do państwa trzeciego ani do organizacji międzynarodowej.

Dane osobowe będą przechowywane do chwili zakończenia sprawy, w której zostały one zebrane, a następnie – w przypadkach, w których wymagają tego przepisy ustawy z dnia 14 lipca 1986 r. o narodowym zasobie archiwalnym i archiwach – przez czas określony w tych przepisach.

Osobie, której dane dotyczą przysługuje prawo do:

- dostępu do danych osobowych; żądania ich sprostowania; ograniczenia przetwarzania, w przypadkach wymienionych w RODO,
- wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

Osobie, której dane dotyczą nie przysługuje prawo do:

- przenoszenia danych, usunięcia danych oraz prawo do wniesienia sprzeciwu.

Informuję, że prawo do sprzeciwu nie przysługuje Pani/Panu ze względu na to, że istnieją ważne, prawnie uzasadnione podstawy do przetwarzania Pani/Pana danych osobowych.

W trakcie przetwarzania danych nie będzie dochodziło do zautomatyzowanego podejmowania decyzji ani do profilowania.

