



Wojskowa
Akademia
Techniczna

Zarządzenie

Rektora Wojskowej Akademii Technicznej
im. Jarosława Dąbrowskiego

WOJSKOWA AKADEMIA TECHNICZNA

Nr WEW/RKR/00154/2018

Wpłynęło 2018-05-24

Zał. Ark. /Str.

nr 15/RKR/2018 z dnia 24 maja 2018 r.

**w sprawie ochrony danych osobowych w Wojskowej Akademii
Technicznej**

Na podstawie art. 66 ust. 2 ustawy z dnia 27 lipca 2005 r. – Prawo o szkolnictwie wyższym (Dz. U. z 2017 r., poz. 2183 z późn. zm.) oraz § 23 ust. 1 Statutu WAT, stanowiącego załącznik do uchwały nr 215/III/2012 Senatu WAT z dnia 29 marca 2012 r. w sprawie uchwalenia Statutu WAT (t.j. obwieszczenie Rektora WAT nr 1/WAT/2017 z dnia 6 lipca 2017 r.), w celu realizacji postanowień 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), zarządza się co następuje:

§ 1

Wprowadza się do użytku:

- 1) *Politykę bezpieczeństwa danych osobowych w Wojskowej Akademii Technicznej*, stanowiącą Załącznik nr 1 do zarządzenia.
- 2) *Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w WAT*, stanowiącą Załącznik nr 2 do zarządzenia.

§ 2

1. Przetwarzanie danych osobowych w Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego (zwanej dalej: „WAT”) służy realizacji zadań i obowiązków wynikających z art. 13 ust. 1 ustawy z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym (Dz. U. z 2017 r., poz. 2183 z późn. zm.).
2. Przetwarzanie danych osobowych w WAT może odbywać się w systemie informatycznym, a także w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych w celu realizacji zadań, o których mowa w ust. 1.
3. Warunki dotyczące sposobu zarządzania, ochrony, a także trybu postępowania w przypadku naruszenia zasad ochrony danych osobowych przetwarzanych przez WAT regulują załączniki nr 1 i 2.
4. Administratorem danych (zwanym dalej: „AD”) jest Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego z siedzibą w Warszawie (kod:

00-908) przy ul. Gen. Witolda Urbanowicza 2, reprezentowana przez JM Rektora;

5. AD odpowiada za procesy prawidłowego zabezpieczenia i ochrony danych osobowych w szczególności:
 - 1) sprawuje ogólny nadzór nad procesem przetwarzania danych osobowych;
 - 2) zapewnia odpowiednie do zagrożeń i kategorii danych objętych ochroną środki techniczne i rozwiązania organizacyjne;
 - 3) wyznacza inspektora ochrony danych;
 - 4) sprawuje kontrolę i nadzór nad przetwarzaniem danych osobowych przez podmioty przetwarzające;
 - 5) zatwierdza procedury prawidłowego przetwarzania danych osobowych;
 - 6) zatwierdza plany sprawdzeń systemu ochrony danych osobowych;
 - 7) podejmuje działania w zakresie bezpieczeństwa danych osobowych.

§ 3

1. Nadzór nad ochroną danych osobowych w WAT sprawuje inspektor ochrony danych (zwany dalej: „IOD”), powołany przez Rektora WAT w drodze decyzji.
2. Inspektor ochrony danych podlega bezpośrednio Rektorowi WAT.
3. W celu prawidłowego przetwarzania danych osobowych IOD powinien być właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
4. IOD pełni funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami.
5. Do zadań IOD w szczególności należy:
 - 1) informowanie AD oraz osób przetwarzających dane osobowe, podmiotów przetwarzających o obowiązkach wynikających z RODO;
 - 2) monitorowanie przestrzegania przepisów RODO, innych przepisów Unii Europejskiej, prawa krajowego oraz wewnętrznych aktów prawnych regulujących ochronę danych osobowych;
 - 3) dokonywanie aktualizacji wewnętrznych aktów prawnych dotyczących ochrony danych osobowych;
 - 4) zapewnienie osobom upoważnionym do przetwarzania danych osobowych zapoznania z przepisami o ochronie danych osobowych;
 - 5) prowadzenie rejestru czynności przetwarzania.
6. AD powierza IOD następujące obowiązki:
 - 1) informowanie AD o przypadkach naruszenia bezpieczeństwa danych osobowych;

- 2) prowadzenie postępowań wyjaśniających w przypadku podejrzenia naruszenia bezpieczeństwa danych osobowych;
 - 3) sprawdzanie jednostek organizacyjnych WAT pod kątem zgodności przetwarzania danych osobowych z obowiązującymi przepisami;
 - 4) udzielanie na wniosek kierowników jednostek organizacyjnych opinii i rekomendacji w zakresie prawidłowego przetwarzania danych osobowych;
 - 5) ocena stanu ochrony danych osobowych w obszarach przetwarzania danych osobowych.
7. AD wspiera wypełnianie obowiązków IOD w szczególności przez zapewnienie zasobów niezbędnych do ich wykonania oraz zapewnienie dostępu do danych osobowych i operacji przetwarzania danych osobowych.
8. IOD jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań.

§ 4

1. Organizację przetwarzania, zapewnienia bezpieczeństwa i ochrony danych osobowych w pionach i jednostkach organizacyjnych AD powierza specjalistom ds. ochrony danych.
2. Specjalistami ds. ochrony danych są:
 - 1) prorektorzy i kierownicy podstawowych jednostek organizacyjnych WAT – w zakresie danych osobowych przetwarzanych w podległych im jednostkach/komórkach organizacyjnych;
 - 2) kanclerz – w zakresie danych osobowych przetwarzanych w jednostkach organizacyjnych jemu podległych oraz w jednostkach organizacyjnych podległych bezpośrednio Rektorowi.

§ 5

Nadzór nad działalnością specjalistów ds. ochrony danych sprawuje AD.

§ 6

1. Specjaliści ds. ochrony danych są odpowiedzialni za wdrożenie w jednostkach organizacyjnych im podległych oraz przez nich nadzorowanych, dokumentacji bezpieczeństwa przetwarzania danych osobowych w WAT oraz realizację obowiązków wynikających z RODO, innych przepisów Unii Europejskiej, prawa krajowego oraz wewnętrznych aktów prawnych regulujących ochronę danych osobowych.
2. Specjalista ds. ochrony danych podejmuje działania mające na celu zwiększenie poziomu ochrony danych osobowych w jednostce organizacyjnej. Szczegółowy zakres zadań został ujęty w Załączniku nr 1 do zarządzenia.
3. Specjalista ds. ochrony danych może powołać lokalnego administratora bezpieczeństwa informacji, (zwanego dalej: „LABI”) oraz powołuje, administratorów systemów informatycznych (zwanymi dalej: „ASI”), w odniesieniu do zarządzanych przez kierowników podległych jednostek organizacyjnych systemów informatycznych, w których przetwarzane są dane osobowe. Szczegółowy zakres zadań dla LABI został ujęty

w Załączniku nr 1 do zarządzenia.

4. W przypadku niepowołania LABI jego obowiązki pełni specjalista ds. ochrony danych.
5. Specjaliści ds. ochrony danych opracują i prześlą do dnia 30 czerwca 2018 r., do IOD niżej wymienione dokumenty:
 - 1) wykaz obszarów przetwarzania danych osobowych - według Formularza nr 12 *Polityki bezpieczeństwa danych osobowych w Wojskowej Akademii Technicznej*;
 - 2) opis przepływu danych osobowych pomiędzy poszczególnymi systemami - według Formularza nr 13 *Polityki bezpieczeństwa przetwarzania danych osobowych w Wojskowej Akademii Technicznej*.
6. Specjalista ds. ochrony danych osobowych odpowiedzialny jest za dany obszar merytoryczny oraz aktywa związane z przetwarzaniem danych osobowych.

§ 7

1. AD uwzględniając charakter, zakres, kontekst i cele przetwarzania danych osobowych oraz ryzyko naruszenia praw lub wolności osób fizycznych, wdraża odpowiednie środki techniczne i organizacyjne w taki sposób, aby przetwarzanie danych odbywało się zgodnie z RODO, innymi przepisami Unii Europejskiej, prawa krajowego oraz wewnętrznymi aktami prawnymi regulującymi ochronę danych osobowych.
2. Do przetwarzania danych osobowych w WAT mogą być dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych.
3. AD jest zobowiązany zapewnić przetwarzanie danych osobowych w WAT zgodnie z prawem.
4. Środki techniczne i organizacyjne obejmują wdrożenie przez AD odpowiednich polityk ochrony danych.

§ 8

1. Za bezpieczeństwo przetwarzania danych osobowych odpowiedzialna jest każda osoba przetwarzająca dane osobowe.
2. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, w trakcie zatrudnienia, a także po ustaniu stosunku służby lub pracy, odwołaniu z pełnionej funkcji, zrealizowaniu umowy lub porozumienia.
3. Osoba upoważniona do przetwarzania danych osobowych wykorzystuje dane osobowe wyłącznie w ramach realizowanych czynności służbowych, zgodnie z przepisami RODO, innymi przepisami Unii Europejskiej, prawa krajowego oraz wewnętrznymi aktami prawnymi regulującymi ochronę danych osobowych.

§ 9

1. Osoby, których dane są przetwarzane w WAT, mają prawo (na warunkach określonych w RODO) do: ochrony danych ich dotyczących, dostępu do treści swoich danych, ich sprostowania, usunięcia, ograniczenia przetwarzania, przenoszenia danych, wniesienia sprzeciwu, cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem, jak również do uzyskiwania informacji o przysługujących im prawach.
2. AD w celu wypełnienia obowiązku informacyjnego wobec osób, których dane osobowe są przetwarzane w WAT, jest zobligowany do podania osobie, której dane dotyczą informacji wskazanych w RODO (tak zwana klauzula informacyjna). Wzór klauzuli informacyjnej określa Formularz nr 1 *Polityki bezpieczeństwa przetwarzania danych osobowych w Wojskowej Akademii Technicznej*.

§ 10

1. Wszystkie dane osobowe, które są przetwarzane przez WAT podlegają ochronie w zakresie poufności, integralności i dostępności.
2. WAT jako administrator danych może udostępniać dane osobowe przetwarzane we własnych zbiorach.
3. Udostępnianie danych nie może naruszać praw i wolności osób, których dane dotyczą i odbywa się na zasadach określonych w przepisach regulujących ochronę danych osobowych oraz Załączniku nr 1 do zarządzenia.
4. Wniosek o udostępnienie danych osobowych stanowi Formularz nr 3 *Polityki bezpieczeństwa przetwarzania danych osobowych w Wojskowej Akademii Technicznej*.

§ 11

W przypadku, gdy przestrzeganie przepisów dotyczących ochrony danych osobowych będzie nasuwać w praktyce wątpliwości lub niejasności, stosownego wyjaśnienia dokonuje IOD. W razie potrzeby wniośkuje do Rektora o nowelizację dokumentacji bezpieczeństwa przetwarzania danych osobowych w WAT.

§ 12

1. Upoważnienia do przetwarzania danych osobowych należy nadać do dnia 31 grudnia 2018 roku (zgodne z zasadami określonymi w Rozdziale IX *Polityki bezpieczeństwa przetwarzania danych osobowych w Wojskowej Akademii Technicznej*).
2. Do dnia 31 grudnia 2018 r. osoby przetwarzające dane osobowe zobowiązane są do złożenia Oświadczenia o zapoznaniu się z przepisami o ochronie danych osobowych, stanowiącym Formularz nr 7 *Polityki bezpieczeństwa przetwarzania danych osobowych w Wojskowej Akademii Technicznej*.
3. Z dniem 1 stycznia 2019 roku wygasają wydane na podstawie dotychczas obowiązujących przepisów upoważnienia do przetwarzania danych osobowych.

§ 13

Tracą moc:

- 1) Zarządzenie Rektora Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego nr 11/RKR/2015 z dnia 16 czerwca 2015 r. w sprawie ochrony danych osobowych przetwarzanych w WAT.
- 2) Zarządzenie Rektora Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego nr 27/RKR/2015 z dnia 30 września 2015 r. w sprawie organizacji prac opracowania i wdrożenia dokumentacji bezpieczeństwa przetwarzania danych osobowych w Wojskowej Akademii Technicznej.
- 3) Zarządzenie Rektora Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego nr 31/RKR/2015 z dnia 18 grudnia 2015 r. w sprawie wprowadzenia do użytku dokumentacji bezpieczeństwa przetwarzania danych osobowych w WAT.

§ 14

Zarządzenie wchodzi w życie z dniem 25 maja 2018 roku.

Rektor



płk dr hab. inż. Tadeusz SZCZUREK prof. WAT

Załącznik nr 1
do zarządzenia nr...¹⁵.../RKR/2018
z dnia...²⁴...maja 2018 r.

**POLITYKA BEZPIECZEŃSTWA DANYCH
OSOBOWYCH
W WOJSKOWEJ AKADEMII TECHNICZNEJ**

Rozdział I Postanowienia ogólne

§ 1

1. Dla utrzymania zgodności z wymaganiami 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), zwane dalej: „RODO” lub „ogólnym rozporządzeniem o ochronie danych” w celu zapewnienia bezpieczeństwa danych osobowych, Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego zwana dalej: „WAT” lub „Wojskową Akademią Techniczną”, dąży do utrzymania wysokiego poziomu bezpieczeństwa danych osobowych przetwarzanych w WAT oraz ograniczenia ryzyka zagrażającego poufności, integralności i dostępności tych danych.
2. Obowiązek ochrony danych osobowych w Wojskowej Akademii Technicznej, wynika z RODO oraz potrzeb zabezpieczenia statutowej działalności WAT, jako publicznej uczelni akademickiej, a także jako jednostki wojskowej.
3. Uznając bezpieczeństwo danych osobowych za priorytet – władze, kierownictwo, wszyscy pracownicy i współpracownicy Wojskowej Akademii Technicznej zobowiązują się do przestrzegania i stosowania zasad wynikających z *Polityki bezpieczeństwa danych osobowych w Wojskowej Akademii Technicznej* zwanej dalej: „Polityką” lub „Polityką bezpieczeństwa danych osobowych”.
4. Dane osobowe mogą być przetwarzane w systemach informatycznych oraz w wersji papierowej.
5. Pod szczególną ochroną pozostają dane szczególnych kategorii, o których mowa w art. 9 ust. 1 RODO, których przetwarzanie jest dopuszczalne tylko w granicach wynikających z przepisów art. 9 ust. 2 RODO.
6. Fakty wystąpienia poważnych naruszeń ochrony danych osobowych powinny skutkować w razie potrzeby zmianami niniejszej Polityki.

§ 2

1. Celem *Polityki bezpieczeństwa danych osobowych w Wojskowej Akademii Technicznej*, jest:
 - 1) zapewnienie odpowiedniego poziomu ochrony przetwarzanych danych osobowych w Wojskowej Akademii Technicznej, poprzez określenie systemu ochrony odpowiedniego do występujących zagrożeń oraz kategorii przetwarzanych danych osobowych objętych ochroną;
 - 2) zapewnienie przetwarzania danych osobowych zgodnie z obowiązującymi przepisami oraz ich ochrona przed udostępnieniem osobom nieupoważnionym, zabranie przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed uszkodzeniem, zniszczeniem lub nieupoważnioną zmianą;
 - 3) określenie oraz wdrożenie i realizacja działań przy wykorzystaniu środków technicznych i organizacyjnych, które zapewnią maksymalny poziom bezpieczeństwa procesu przetwarzania danych osobowych;

- 4) kształtowanie u osób, które przetwarzają dane osobowe, odpowiedniej świadomości w zakresie ochrony oraz bezpieczeństwa przetwarzanych danych.
2. Polityka bezpieczeństwa danych osobowych odnosi się całościowo do problematyki zabezpieczenia danych osobowych Wojskowej Akademii Technicznej, zarówno do danych przetwarzanych w formie papierowej jak i danych przetwarzanych przy użyciu systemu informatycznego.
3. Polityka jest realizowana na każdym etapie przetwarzania danych osobowych i ma zastosowanie w stosunku do studentów, doktorantów, pracowników, żołnierzy, stażystów, praktykantów, wolontariuszy oraz osoby realizujące zadania na rzecz Wojskowej Akademii Technicznej na podstawie umowy.
4. Polityka bezpieczeństwa danych osobowych w WAT jest zbiorem zasad i procedur obowiązujących przy przetwarzaniu danych osobowych we wszystkich zbiorach administrowanych przez Wojskową Akademię Techniczną obowiązuje, także przy przetwarzaniu danych osobowych poza zbiorami danych.
5. Polityka służy zapewnieniu wysokiego poziomu bezpieczeństwa danych osobowych przetwarzanych w zbiorach takich jak: kartoteki, skorowidze, księgi, wykazy i inne zbiory ewidencyjne oraz w systemach informatycznych.
6. Polityka ma zastosowanie we wszystkich jednostkach organizacyjnych WAT.
7. Polityka dotyczy wszystkich danych osobowych przetwarzanych w WAT, niezależnie od formy ich przetwarzania (np. zbiory ewidencyjne, systemy informatyczne) oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych.
8. Polityka bezpieczeństwa danych osobowych jest dokumentem, który ze względu na zmieniające się zagrożenia przetwarzania danych osobowych i zmiany prawa, podlega na bieżąco uaktualnianiu w zakresie procedur ochrony, oprogramowania i innych parametrów stosowanych przy przetwarzaniu danych osobowych.
9. Realizując Politykę bezpieczeństwa danych osobowych, WAT udostępnia przetwarzane na jej obszarze dane osobowe wyłącznie osobom do tego upoważnionym na mocy przepisów prawa i uregulowań wewnętrznych. Upoważnienie to wynikać może w szczególności:
 - 1) z charakteru i zakresu obowiązków pracy wykonywanej na danym stanowisku pracy;
 - 2) z odrębnego imiennego upoważnienia do dostępu do danych osobowych.

§ 3

Polityka bezpieczeństwa danych osobowych jest zbiorem procedur zawierających zasady i definicje związane z ochroną danych osobowych przetwarzanych w Wojskowej Akademii Technicznej.

§ 4

1. Zakres przedmiotowy Polityki bezpieczeństwa danych osobowych obejmuje wszystkie dane osobowe przetwarzane w Wojskowej Akademii Technicznej.
2. W zakresie podmiotowym Polityka bezpieczeństwa danych osobowych obejmuje wszystkie osoby posiadające prawo do kontroli przetwarzania danych osobowych i wykonujące zadania na rzecz Wojskowej Akademii Technicznej, w tym między

innymi: studentów, doktorantów, pracowników, żołnierzy, stażystów, praktykantów, wolontariuszy oraz osoby realizujące zadania na rzecz Wojskowej Akademii Technicznej na podstawie umowy.

3. Zarządzanie bezpieczeństwem danych osobowych stanowi proces ciągły, na który składają się takie elementy, jak: identyfikacja oraz analiza zagrożeń i ryzyka, stosowanie odpowiednich zabezpieczeń, monitorowanie, wdrażanie i eksploatacja zabezpieczeń, a także wykrywanie i reagowanie na incydenty.

§ 5

1. Utrzymanie bezpieczeństwa ochrony danych osobowych przetwarzanych przez Wojskową Akademię Techniczną rozumiane jest jako dążenie do zapewnienia ich poufności, integralności i dostępności na poziomie wymaganym przepisami prawa w zakresie ochrony danych osobowych. Miarą bezpieczeństwa jest poziom ryzyka utraty integralności, dostępności lub poufności danych osobowych osiągany poprzez podejmowanie działań minimalizujących to ryzyko stosownie do wyników przeprowadzonych analiz ryzyka.
2. Inspektor ochrony danych sprawując nadzór nad procesem przetwarzania danych osobowych wyznacza kierunki rozwoju oraz zasady działania i doskonalenia prawidłowego procesu przetwarzania danych osobowych.
3. Polityka bezpieczeństwa danych osobowych jest:
 - 1) podstawą do tworzenia dokumentów zawierających wymagania bezpieczeństwa dla danych osobowych;
 - 2) podstawą określenia warunków, jakie muszą spełniać systemy informatyczne.
4. Polityka bezpieczeństwa danych osobowych gwarantuje danym osobowym przetwarzanym w Wojskowej Akademii Technicznej:
 - 1) **poufność** – właściwość zapewniająca, że dane nie są udostępniane osobom nieupoważnionym;
 - 2) **integralność** – właściwość polegająca na tym, że dane nie zostały zmodyfikowane lub zniszczone w sposób nieuprawniony;
 - 3) **dostępność** – rozumie się przez to właściwość zapewniającą, że dane są osiągalne i możliwe do wykorzystania na żądanie, w założonym czasie, przez uprawnioną osobę lub podmiot;
 - 4) **rozliczalność** – właściwość zapewniająca, zapewnieniu, że działania podmiotu mogą być przy pisane w sposób jednoznaczny tylko temu podmiotowi;
 - 5) **ciągłość** – zdolność do niezakłóconego przetwarzania danych osobowych, bez przerw uniemożliwiających ich udostępnianie osobom upoważnionym;
 - 6) **przejrzystość przetwarzania** – dane osobowe mają być przetwarzane w zrozumiałej formie dla osób, których dotyczą.
5. Polityka bezpieczeństwa ochrony danych osobowych zakłada ochronę danych przetwarzanych w Wojskowej Akademii Technicznej, w szczególności przed ich nieuprawnionym dostępem, kradzieżą, uszkodzeniem lub zakłóceniami.

§ 6

1. Cele określone w niniejszej Polityce realizowane są przez:

- 1) określenie funkcji i odpowiedzialności w zakresie ochrony danych osobowych;
 - 2) stosowanie przez wszystkie osoby przetwarzające dane osobowe w Wojskowej Akademii Technicznej procedur obowiązujących w niniejszej Polityce;
 - 3) przegląd i aktualizację Polityki bezpieczeństwa danych osobowych;
 - 4) ciągłe podnoszenie świadomości osób przetwarzających dane osobowe w Wojskowej Akademii Technicznej w zakresie możliwych zagrożeń i bezpieczeństwa danych osobowych (np. poprzez prowadzenie szkoleń);
 - 5) ciągłe doskonalenie systemu ochrony danych osobowych w Wojskowej Akademii Technicznej.
2. Administrator zapewnia warunki umożliwiające realizację i egzekwowanie określonych w Polityce ochrony danych osobowych celów.
 3. Nadzór nad przestrzeganiem Polityki bezpieczeństwa ochrony danych osobowych sprawuje inspektor ochrony danych.
 4. Każda osoba przetwarzająca dane osobowe jest zobowiązana do zapoznania się z Polityką.

Rozdział II Podstawowe definicje

§ 7

Przez użyte w niniejszej Polityce określenia rozumie się:

- 1) **administrator** – zwany dalej: „administratorem danych” lub „AD”, to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych (Wojskowa Akademia Techniczna reprezentowana przez JM Rektora);
- 2) **administrator systemu informatycznego** – zwany dalej: „ASI” – osoba odpowiedzialna za zapewnienie właściwego funkcjonowania systemu teleinformatycznego, przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu, przeciwdziałanie dostępowi osób trzecich do systemu oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w tym systemie;
- 3) **anonimizacja danych** – rozumie się przez to nieodwracalny proces polegający na tym, by nie istniała już możliwość wykorzystania danych do zidentyfikowania osoby fizycznej za pomocą „wszystkich sposobów, jakimi można się posłużyć”;
- 4) **dane osobowe** – oznaczają 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 osoby fizycznej;

- 5) **elektroniczny nośnik** – elektroniczne urządzenie, na którym przechowuje się dane osobowe w celu ich ponownego odtworzenia w systemie informatycznym;
- 6) **hasło** – ciąg znaków literowych, cyfrowych lub innych specjalnych znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
- 7) **identyfikator użytkownika/login** – ciąg znaków literowych, cyfrowych lub innych specjalnych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych w systemie informatycznym;
- 8) **incydent** – rozumie się przez to naruszenie bezpieczeństwa danych osobowych;
- 9) **instrukcja/procedura** – dokument opisujący sposób postępowania i warunki realizacji jakiegoś działania lub grupy działań (procesów);
- 10) **inspektor ochrony danych** – zwany dalej: „IOD” – rozumie się przez to osobę wyznaczoną przez administratora w celu wsparcia AD w nadzorowaniu i przestrzeganiu zasad ochrony danych w Wojskowej Akademii Technicznej;
- 11) **kierownik jednostki organizacyjnej** – na potrzeby niniejszej Polityki zgodnie z Regulaminem organizacyjnym Wojskowej Akademii Technicznej oznacza: dziekana, dyrektora lub kierownika innej, niebędącej wydziałem jednostki organizacyjnej WAT, a także kierownika jednostki administracji centralnej – kierownika biura lub kierownika działu;
- 12) **naruszenie ochrony danych osobowych** – oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia lub zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych, przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
- 13) **obszar przetwarzania danych** – oznacza wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
- 14) **odbiorca** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią;
- 15) **opis przepływu danych** – oznacza opis przepływu danych między podmiotami przetwarzania przy wykorzystaniu systemów informatycznych;
- 16) **organ nadzorczy** – oznacza niezależny organ publiczny, ustanowiony przez państwo członkowskie UE;
- 17) **osoba nieuprawniona** – osoba, która nie powinna mieć dostępu do danych osobowych przetwarzanych w Wojskowej Akademii Technicznej;
- 18) **podmiot przetwarzający** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Wojskowej Akademii Technicznej;
- 19) **pracownik** – osoba pozostająca w stosunku pracy z Wojskową Akademią Techniczną na podstawie umowy o pracę, a także osoba wykonująca pracę i czynności na podstawie umów innych niż umowa o pracę (w tym umów

cywilnoprawnych oraz praktykanci, stażyści, wolontariusze) oraz żołnierze zawodowi pełniący zawodową służbę wojskową w WAT;

- 20) **profilowanie** – oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
- 21) **przetwarzanie** – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak 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 niszczenie;
- 22) **pseudonimizacja** – przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
- 23) **specjalista ds. ochrony danych** – zgodnie z zarządzeniem Rektora, prorektorzy, kanclerz, kierownicy podstawowych jednostek organizacyjnych;
- 24) **system informatyczny** – oznacza zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
- 25) **środki techniczne i organizacyjne** – oznaczają środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych;
- 26) **usuwanie danych** – oznacza zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą – anonimizacja;
- 27) **użytkownik** – osoba posiadająca upoważnienie do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu;
- 28) **zabezpieczenie danych** – oznacza wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
- 29) **zagrożenie** – rozumie się przez to potencjalną możliwość wystąpienia incydentu;
- 30) **zasoby danych** – inaczej aktywa, wszystko co ma wartość dla WAT i służy przetwarzaniu informacji w tym dane osobowe przetwarzane w Wojskowej Akademii Technicznej;
- 31) **zbiór danych** – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten

jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

- 32) **zgoda osoby, której dane dotyczą** – oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, w którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

Rozdział III Struktura organizacyjna

§ 8

Administrator danych

1. Administratorem danych jest Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego z siedzibą w Warszawie (kod: 00-908) przy ul. Gen. Witolda Urbanowicza 2, reprezentowana przez JM Rektora.
2. AD odpowiada za procesy prawidłowego zabezpieczenia i ochrony danych osobowych, w tym za podejmowanie najważniejszych decyzji w celu zapewnienia skuteczności i doskonalenia ochrony danych osobowych, w szczególności:
 - 1) sprawuje ogólny nadzór nad procesem przetwarzania danych osobowych;
 - 2) zapewnia odpowiednie do zagrożeń i kategorii danych objętych ochroną środki techniczne i rozwiązania organizacyjne;
 - 3) wyznacza inspektora ochrony danych;
 - 4) sprawuje kontrolę i nadzór nad przetwarzaniem danych osobowych przez podmioty, którym dane zostały udostępnione lub powierzone;
 - 5) zatwierdza procedury prawidłowego przetwarzania danych osobowych;
 - 6) zatwierdza plany sprawdzeń systemu ochrony danych osobowych;
 - 7) podejmuje strategiczne decyzje w zakresie bezpieczeństwa danych osobowych.
3. Wojskowa Akademia Techniczna – zgodnie z przepisami ogólnego rozporządzenia o ochronie danych, jako administrator – jest zobowiązana zabezpieczyć oraz chronić dane osobowe i w tym zakresie deklaruje pełne wsparcie dla uzasadnionych i niezbędnych działań podejmowanych, w celu ochrony przetwarzanych danych osobowych. Realizując powyższy obowiązek, niezbędne jest zachowanie szczególnej staranności w celu ochrony interesów i praw osób, których dane dotyczą, a w szczególności zapewnienia, aby dane osobowe były:
 - 1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);
 - 2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami. Dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane za niezgodne z pierwotnymi celami („ograniczenie celu”);
 - 3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);

- 4) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);
 - 5) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane („ograniczenie przechowywania”);
 - 6) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”).
4. Administrator musi być w stanie wykazać przestrzeganie zasad opisanych w ust. 3 pkt 1-6 („rozliczalność”).
 5. Administrator danych wdraża i wprowadza do stosowania w Wojskowej Akademii Technicznej, kodeksy postępowania zatwierdzone przez organ nadzorczy. Kodeksy postępowania mają na celu pomoc we właściwym stosowaniu ogólnego rozporządzenia o ochronie danych.
 6. Administrator danych wdraża w Wojskowej Akademii Technicznej rekomendacje zamieszczone przez organ nadzorczy na stronie urzędu.
 7. Administrator danych przy współpracy z IOD prowadzi rejestr czynności przetwarzania danych. Administrator danych, po konsultacji z IOD dokonuje oceny skutków dla ochrony danych.

§ 9

Inspektor ochrony danych

1. Inspektor ochrony danych zostaje wyznaczony przez Rektora Wojskowej Akademii Technicznej i wpisany do prowadzonego przez Prezesa Urzędu Ochrony Danych Osobowych rejestru inspektorów ochrony danych osobowych. IOD jest odpowiedzialny za nadzór i bezpieczeństwo danych osobowych przetwarzanych w WAT.
2. IOD odpowiada za nadzór nad funkcjonowaniem i efektywnością procesów prawidłowego przetwarzania danych osobowych, w szczególności:
 - 1) nadzoruje działania wdrożeniowe, korygujące i zapobiegawcze związane z bezpieczeństwem danych osobowych;
 - 2) zapewnia bieżący nadzór nad przestrzeganiem ochrony danych osobowych;
 - 3) przeprowadza kontrole/audyty minimum raz w roku w wybranych jednostkach organizacyjnych WAT oraz dokumentuje ich wykonanie sprawozdaniami, które składa administratorowi danych;
 - 4) zapewnia szkolenia w zakresie ochrony danych osobowych;
 - 5) prowadzi rejestr czynności przetwarzania danych osobowych oraz rejestr wszystkich kategorii czynności przetwarzania danych osobowych dokonywanych w imieniu administratora;
 - 6) przygotowuje przegląd i aktualizację dokumentacji ochrony danych

osobowych;

- 7) przedstawia AD sprawozdania dotyczące funkcjonowania systemu ochrony danych osobowych w Wojskowej Akademii Technicznej;
- 8) koordynuje działania pomiędzy jednostkami organizacyjnymi w zakresie ochrony danych osobowych;
- 9) nadzoruje ocenę skuteczności wdrożonych zabezpieczeń oraz realizację działań korygujących i zapobiegawczych dotyczących ochrony danych osobowych;
- 10) prowadzi rejestr udostępnionych danych;
- 11) w razie potrzeby opracowuje wytyczne/zalecenia/procedury prawidłowego przetwarzania danych osobowych;
- 12) wydaje opinie w zakresie dotyczącym przetwarzania danych osobowych;
- 13) prowadzi rejestr naruszeń (incydentów);
- 14) współpracuje i pełni funkcję kontaktową dla organu nadzorczego w kwestiach związanych z ochroną danych osobowych, w tym z uprzednimi konsultacjami;
- 15) informuje administratora, podmiot przetwarzający oraz osoby, które przetwarzają dane osobowe o ich obowiązkach i doradza im w zakresie ochrony danych osobowych;
- 16) prowadzi działania zwiększające świadomość oraz szkolenia użytkowników uczestniczących w operacjach przetwarzania;
- 17) udziela na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitoruje jej wykonanie.

§ 10

1. IOD prowadzi rejestr czynności przetwarzania danych, obejmujący następujące informacje gromadzone przez WAT jako administratora:
 - 1) oznaczenie administratora danych, adres jego siedziby, oznaczenie inspektora ochrony danych;
 - 2) czynność przetwarzania danych osobowych;
 - 3) cel przetwarzania danych osobowych;
 - 4) podstawa prawna upoważniająca do przetwarzania danych osobowych;
 - 5) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
 - 6) zakres danych osobowych;
 - 7) sposób zbierania danych osobowych;
 - 8) fizyczna lokalizacja przetwarzania danych osobowych;
 - 9) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
 - 10) przekazanie danych osobowych do państwa trzeciego lub organizacji

międzynarodowej w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazania, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń;

- 11) planowany termin usunięcia poszczególnych kategorii danych;
 - 12) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO;
 - 13) dane podmiotu, któremu powierzono przetwarzanie danych.
2. Rejestr czynności przetwarzania danych osobowych jest tworzony w oparciu o informacje ze wszystkich jednostek organizacyjnych/komórek WAT. Wzór zgłoszenia do rejestru czynności przetwarzania danych osobowych stanowi Formularz nr 9 Polityki.

§ 11

IOD prowadzi rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, zawierający następujące informacje gromadzone przez WAT jako podmiot przetwarzający:

- 1) imię i nazwisko lub nazwa oraz dane kontaktowe administratora w imieniu którego działa WAT, (a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego);
- 2) dane kontaktowe inspektora ochrony danych;
- 3) kategorie przetwarzania dokonywanych w imieniu administratora;
- 4) przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazania, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń;
- 5) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO;
- 6) data, numer umowy głównej/o powierzeniu danych osobowych (jeżeli podpisano) wraz z datami ich podpisania;
- 7) czas trwania umowy;
- 8) zasady zakończenia współpracy (np. zniszczenie danych, oddanie danych).

§ 12

Rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora innego niż WAT jest tworzony w oparciu o informacje ze wszystkich jednostek organizacyjnych/komórek WAT, które w wyniku zawartych umów/umów powierzenia danych osobowych i porozumień przetwarzają dane osobowe innych podmiotów (administratorów) niż WAT, pełniąc role podmiotu przetwarzającego.

§ 13

Wzór zgłoszenia do rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora innego niż WAT stanowi Formularz nr 10 Polityki.

§ 14

W czasie nieobecności IOD jego obowiązki pełni osoba wyznaczona przez Rektora WAT.

§ 15

Wszystkie osoby przetwarzające dane osobowe w WAT bez względu na zajmowane stanowisko, rodzaj i miejsce wykonywania pracy oraz charakter stosunku zatrudnienia, zobowiązani są do współdziałania z IOD w zakresie przestrzegania zasad ochrony danych osobowych w WAT.

§ 16

Specjalista ds. ochrony danych

1. Organizację przetwarzania danych osobowych oraz zapewnienie ich bezpieczeństwa i ochrony w pionach i jednostkach organizacyjnych, administrator danych powierza „specjalistom ds. ochrony danych osobowych”.
2. Specjalistami ds. ochrony danych są:
 - 1) prorektorzy i kierownicy podstawowych jednostek organizacyjnych WAT w zakresie danych osobowych przetwarzanych w podległych im jednostkach/komórkach organizacyjnych;
 - 2) kanclerz – w zakresie danych osobowych przetwarzanych w jednostkach organizacyjnych jemu podległych oraz w jednostkach organizacyjnych podległych bezpośrednio Rektorowi.
3. Specjalista ds. ochrony danych podejmuje działania mające na celu zwiększenie poziomu ochrony danych osobowych w jednostce organizacyjnej oraz odpowiada za zarządzanie procesami przetwarzania danych osobowych w danym obszarze merytorycznym.
4. Specjalista ds. ochrony danych może powołać lokalnego administratora bezpieczeństwa informacji, zwanego dalej: „LABI”. W przypadku niepowołania LABI obowiązki jego pełni specjalista ds. ochrony danych.
5. LABI zapewnia przestrzeganie obowiązujących zasad przetwarzania i ochrony danych osobowych w jednostkach organizacyjnych podległych specjalście ds. ochrony danych (zakres obowiązków LABI przedstawia Załącznik nr 3 do Polityki).
6. Specjalista ds. ochrony danych odpowiedzialny jest za dany obszar merytoryczny oraz aktywa związane z przetwarzaniem danych osobowych.
7. Nadzór nad działalnością specjalistów ds. ochrony danych sprawuje administrator danych.
8. Do głównych zadań specjalisty ds. ochrony danych między innymi należy:
 - 1) wspieranie IOD w nadzorowaniu zasad ochrony danych osobowych w danym obszarze merytorycznym;
 - 2) przy współdziałaniu z IOD - organizowanie szkolenia osób upoważnionych do przetwarzania danych osobowych z obowiązujących przepisów, zasad przetwarzania i ich ochrony oraz odpowiedzialności za ich naruszenie, a w szczególności za nieuprawnione ujawnienie danych osobowych zarówno celowe jak i w wyniku działań nieumyślnych;

- 3) zapewnienie przestrzegania przez osoby upoważnione do przetwarzania danych osobowych w jednostce organizacyjnej przepisów regulujących ochronę danych osobowych;
- 4) bieżąca współpraca z IOD oraz zgłaszanie mu problemów wynikających z realizacji zadań w jednostce organizacyjnej w zakresie ochrony danych osobowych;
- 5) decydowanie o zastosowaniu środków technicznych i organizacyjnych mających na celu zapewnienie ochrony danych osobowych w nadzorowanym obszarze, adekwatnych do występujących zagrożeń;
- 6) określenie wartości aktywów danych osobowych i analizy ryzyka utraty bezpieczeństwa danych osobowych;
- 7) kontrola dostępu do zasobów danych osobowych, w tym systemów informatycznych;
- 8) decydowanie o narzędziach, metodach, miejscu przetwarzania, przechowywania, wytwarzania i niszczenia danego zasobu danych osobowych oraz o tym, które osoby mają do nich dostęp;
- 9) wyznaczenie administratora systemu informatycznego w odniesieniu do zarządzanych przez kierowników podległych jednostek organizacyjnych systemów informatycznych, w których przetwarzane są dane osobowe:
 - a) autonomicznych przetwarzających dane na potrzeby podległej jednostki organizacyjnej,
 - b) rozproszonych, rozległych, zarządzanych centralnie zabezpieczających przetwarzanie danych na potrzeby podległej i innych jednostek (komórek) organizacyjnych WAT,
 - c) zewnętrznych, których użytkownikiem jest WAT,
- 10) określenie zakresów obowiązków dla ASI oraz uzupełnienie zakresów obowiązków pracowniczych;
- 11) nadzorowanie wykonywania zadań przez LABI oraz ASI oraz informowanie IOD o ich powołaniu;
- 12) zgłaszanie IOD potrzeb szkoleniowych w zakresie ochrony danych osobowych;
- 13) dopuszczenie do przetwarzania danych osobowych wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych i zapewnienie adekwatnego dostępu do danych i urządzeń do prawidłowego wykonywania obowiązków;
- 14) przetwarzanie danych osobowych adekwatnych do określonego celu przetwarzania oraz stosowanie zasady minimalizacji danych;
- 15) udzielanie odpowiedzi na wnioski o udostępnienie danych osobowych oraz prowadzenie rejestru udostępnionych danych zgodnie z Formularzem nr 4 Polityki;
- 16) prowadzenie i aktualizacja rejestrów czynności przetwarzania danych osobowych w jednostce organizacyjnej zgodnie z Formularzem nr 9, 10 Polityki;

- 17) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych w danej jednostce organizacyjnej WAT zgodnie z Formularzem nr 11 Polityki;
- 18) prowadzenie wykazu obszarów przetwarzania danych osobowych oraz opisu przepływu danych osobowych pomiędzy poszczególnymi systemami zgodnie z Formularzem nr 12 oraz 13 Polityki;
- 19) zgłaszanie IOD danych do rejestru czynności przetwarzania danych oraz informacji dotyczących wszelkich zmian w jego zawartości;
- 20) prowadzenie rejestru naruszeń (incydentów);
- 21) przekazywanie IOD wniosków o udostępnianie danych osobowych innemu podmiotowi niż uprawniony na podstawie przepisów prawa w celu uzyskania opinii w sprawie udostępnienia danych;
- 22) identyfikacja ryzyka procesu przetwarzania danych osobowych i dokonanie (w uzasadnionych przypadkach) oceny skutków dla ochrony danych osobowych;
- 23) sprawowanie nadzoru nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe.

§ 17

Administrator systemu informatycznego

1. Administrator systemu informatycznego to osoba nadzorująca pracę systemu informatycznego.
2. ASI jest odpowiedzialny za bezpieczeństwo systemu informatycznego.
3. Do głównych zadań ASI należy, w szczególności:
 - 1) zapewnienie ciągłości działania i bezpieczeństwa systemu, w tym wykonywania kopii zapasowych;
 - 2) zarządzanie uprawnieniami w systemie informatycznym;
 - 3) administrowanie, konfigurowanie, aktualizowanie oraz testowanie zmiany w systemie informatycznym;
 - 4) monitorowanie systemu i przekazywanie informacji o zagrożeniach IOD;
 - 5) wsparcie merytoryczne IOD w zakresie przeprowadzanych audytów dotyczących przetwarzania danych osobowych z wykorzystaniem systemów informatycznych oraz prowadzenie szkoleń z zasad przetwarzania danych osobowych w systemach informatycznych;
 - 6) wykonywanie bieżących i okresowych przeglądów technicznych;
 - 7) aktywny udział w procesie reagowania na podatności i incydenty ochrony danych osobowych w systemach informatycznych oraz usuwaniu ich skutków.
4. Szczegółowy zakres zadań ASI określa specjalista ds. ochrony danych.

Rozdział IV Podstawowe zasady ochrony danych osobowych

§ 18

1. **Zasada odpowiedzialności za zasoby** – użytkownik jest odpowiedzialny za przetwarzane dane. Podczas ich przetwarzania przestrzega procedur bezpieczeństwa w celu zapewnienia dostępności, poufności oraz integralności powierzonych danych.
2. **Zasada ochrony informacji/dokumentów** – zabronione jest kopiowanie i wynoszenie dokumentów służbowych (oryginałów, kopii, wersji elektronicznych) oraz ich przesyłanie drogą elektroniczną w innym celu niż służbowy.
3. **Zasada wiedzy koniecznej** – ograniczenie dostępu użytkownika jedynie do tych informacji, które są niezbędne do wykonywania obowiązków lub zadań.
4. **Zasada zamkniętego pomieszczenia** – osoby nieuprawnione nie pozostają same w pomieszczeniu pod nieobecność pracownika Wojskowej Akademii Technicznej. Drzwi zamykane są na klucz, który pozostaje pod nadzorem (nie w zamku).
5. **Zasada czystego biurka** – dokumenty papierowe oraz nośniki danych, nie pozostają bez nadzoru.
6. **Zasada prywatności kont w systemach** – praca w systemach informatycznych odbywa się na kontach przypisanych danemu użytkownikowi. Zabronione jest udostępnianie kont osobom, które nie zostały do nich przypisane.
7. **Zasada poufności haseł i kodów dostępu** – zachowanie poufności i nieprzekazywanie osobom nieuprawnionym haseł i kodów dostępu.
8. **Zasada czystej tablicy** – po zakończonym spotkaniu w pomieszczeniach ogólnodostępnych, wszystkie materiały zostają uprzątnięte, a tablice wyczyszczone.
9. **Zasada czystego ekranu** – użytkownik blokuje komputer przed każdym opuszczeniem pomieszczenia. W przypadku dłuższej nieobecności w pomieszczeniu konieczne jest wylogowanie z systemu.
10. **Zasada czystego pulpitu** – na pulpicie komputera mogą znajdować się jedynie ikony standardowego oprogramowania, aplikacji służbowych oraz pliki i skróty do folderów pod warunkiem, że w nazwie nie zawierają informacji, które mogą zostać w sposób niekontrolowany ujawnione.
11. **Zasada czystych drukarek** – dokumenty są zabierane z drukarek zaraz po ich wydrukowaniu. W szczególności zasada ta dotyczy dokumentów drukowanych w drukarkach znajdujących się w innym pomieszczeniu.
12. **Zasada czystego kosza** – do kosza wyrzucane są dokumenty, z których usunięto dane umożliwiające zapoznanie się z treścią dokumentów papierowych lub z odczytem danych z nośników elektronicznych.
13. **Zasada niszczenia** – dokumenty zawierające dane osobowe należy niszczyć za pomocą niszcarki dokumentów.

14. **Zasada legalności oprogramowania** – zabronione jest samodzielne instalowanie oprogramowania i przechowywanie na komputerze treści naruszających prawa autorskie oraz innych nielegalnych treści.
15. **Zasada minimalizacji danych** – dane osobowe powinny być adekwatne, stosowne do celu przetwarzania danych osobowych oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

Rozdział V

Przetwarzanie i powierzenie przetwarzania danych

§ 19

Przesłanki legalności przetwarzania danych

1. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:
 - 1) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów:
 - a) zgoda na przetwarzanie danych osobowych powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności, która wyraża odnoszące się do określonej sytuacji dobrowolne, świadome i jednoznaczne przyzwolenie osoby, której dane dotyczą, na przetwarzanie dotyczących jej danych osobowych. Zgoda może przyjąć formę pisemnego (w tym elektronicznego) oświadczenia, może polegać na zaznaczeniu okienka wyboru podczas przeglądania strony internetowej,
 - b) zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, potrzebna jest odrębna zgoda na wszystkie te cele. Jeżeli osoba, której dane dotyczą, ma wyrazić zgodę w odpowiedzi na elektroniczne zapytanie, zapytanie takie musi być jasne, zwięzłe i nie zakłócać niepotrzebnie korzystania z usług, której dotyczy,
 - c) zgoda na przetwarzanie danych osobowych może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania,
 - d) zgoda na przetwarzanie danych osobowych może być odwołana w każdym czasie. W przypadku odwołania zgody na przetwarzanie danych osobowych, administrator danych obowiązany jest usunąć wszystkie dane osoby, która zgodę cofnęła, chyba, że istnieje podstawa prawna upoważniająca Wojskową Akademię Techniczną do dalszego przetwarzania tych danych dla celów innych, niż wskazany w cofniętej zgodzie,
 - e) przykładowy wzór określający treść zgody stanowi Formularz nr 2 załączony do niniejszej Polityki,
 - 2) jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
 - 3) jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;

- 4) jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej;
 - 5) jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
 - 6) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.
2. W przypadku istniejących wątpliwości co do legalności przetwarzania danych niedozwolone jest ich dalsze przetwarzanie, poza przechowywaniem, do czasu rozstrzygnięcia prawnie uzasadnionej wątpliwości.
 3. Szczegółowe zasady oraz obowiązki dotyczące legalnego przetwarzania danych określa RODO.

§ 20

Powierzenie przetwarzania danych osobowych

1. Wojskowa Akademia Techniczna może powierzyć przetwarzanie danych osobowych innemu podmiotowi w drodze umowy zawartej na piśmie.
2. Umowa powierzenia przetwarzania danych osobowych powinna określać między innymi:
 - 1) administratora danych;
 - 2) przedmiot przetwarzania;
 - 3) czas trwania przetwarzania;
 - 4) charakter przetwarzania;
 - 5) cel przetwarzania;
 - 6) rodzaj danych osobowych;
 - 7) kategorie osób, których dane dotyczą;
 - 8) obowiązki i prawa administratora;
 - 9) sposób wykonania umowy w zakresie przetwarzania danych osobowych;
 - 10) określenie odpowiedzialności podmiotu przetwarzającego;
 - 11) wskazanie, że przetwarzanie odbywa się na wyłączone udokumentowane polecenie administratora;
 - 12) zapewnienie, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy, lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
 - 13) oświadczenie podmiotu przetwarzającego, że posiada niezbędne wymagania przepisami prawa środki ochrony fizycznej i organizacyjnej, mające na celu zapewnienie zgodności przetwarzania danych z przepisami;
 - 14) zobowiązanie podmiotu przetwarzającego do przestrzegania warunków korzystania z usług innego podmiotu przetwarzającego;

- 15) obowiązki dotyczące zgłaszania naruszeń ochrony danych osobowych;
 - 16) zobowiązanie do zwrotu lub usunięcia wszelkich danych osobowych oraz usunięcie wszelkich istniejących kopii danych;
 - 17) zobowiązanie podmiotu przetwarzającego do udostępnienia administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w art. 28 RODO oraz umożliwienie AD do przeprowadzenia kontroli prawidłowości przetwarzania danych osobowych.
3. Podmiot, z którym podpisywana jest umowa, obowiązany jest przed rozpoczęciem przetwarzania danych osobowych podjąć środki organizacyjne i techniczne zapewniające ochronę danych osobowych adekwatną do stopnia ryzyka naruszenia praw osób, których dane dotyczą.
 4. Podmiot, któremu powierzono przetwarzanie danych ponosi odpowiedzialność za przetwarzanie danych niezgodne z umową.
 5. Każda umowa powierzenia przetwarzania danych osobowych przed jej podpisaniem powinna zostać zaopiniowana przez Radcę Prawnego z Sekcji Obsługi Prawnej oraz IOD.
 6. Wzór umowy powierzenia przetwarzania danych stanowi Formularz nr 14 Polityki.

Rozdział VI

Obowiązek informacyjny

§ 21

1. Obowiązek informacyjny należy zrealizować z chwilą chęci pozyskiwania danych od osób, których dane dotyczą. Niezbędnych informacji Wojskowa Akademia Techniczna udziela na piśmie lub w inny sposób (w tym także elektronicznie).
2. Wojskowa Akademia Techniczna gromadząc dane od osoby, której dane dotyczą oraz z innych źródeł spełnia obowiązek informacyjny przez:
 - 1) w przypadku zbierania danych od osoby, której dane dotyczą;
 - a) podanie adresu swojej siedziby i pełnej nazwy,
 - b) podanie danych kontaktowych IOD,
 - c) określenie celów przetwarzania danych osobowych oraz informacji o podstawie prawnej przetwarzania,
 - d) (gdy ma to zastosowanie) informowanie o prawnie uzasadnionych interesach realizowanych przez AD lub przez stronę trzecią,
 - e) (gdy ma to zastosowanie) informacje o odbiorcach danych osobowych lub kategoriach odbiorców,
 - f) (gdy ma to zastosowanie) informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej,
 - g) informację o okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe należy poinformować o kryteriach ustalenia tego okresu,
 - h) informacje o prawie żądania od AD dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub

ograniczenia przetwarzania, a także o prawie do wniesienia sprzeciwu wobec przetwarzania oraz o prawie do przenoszenia danych,

- i) informacje o prawie do cofnięcia zgody w dowolnym momencie (jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a RODO) bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
 - j) informację o prawie wniesienia skargi do organu nadzorczego,
 - k) informację czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,
 - l) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu,
- 2) w przypadku zbierania danych nie od osoby, której dane dotyczą dodatkowo należy poinformować tę osobę o:
- a) źródle pochodzenia danych, a jeżeli ma to zastosowanie – informacji czy dane pochodzą ze źródeł publicznie dostępnych,
 - b) celu przetwarzania danych innym niż cel, w którym dane zostały zebrane pierwotnie.
3. Przejrzystość i tryb korzystania z praw osób, których dane dotyczą:
- 1) osoba, której dane dotyczą, jest uprawniona do uzyskania potwierdzenia, czy są przetwarzane dane jej dotyczące, jeżeli ma to miejsce jest uprawniona do uzyskania dostępu do nich oraz uzyskania określonych w ust. 2 pkt 1 informacji;
 - 2) Wojskowa Akademia Techniczna na żądanie osoby, której dane dotyczą dostarcza kopię danych osobowych podlegających przetwarzaniu;
 - 3) w przypadkach uzasadnionej wątpliwości co do tożsamości osoby składającej żądanie Wojskowa Akademia Techniczna może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości.
4. W celu spełnienia obowiązku informacyjnego należy posłużyć się klauzulą informacyjną. Wzór klauzuli informacyjnej stanowi Formularz nr 1 Polityki.

Rozdział VII

Udostępnianie danych osobowych

§ 22

- 1. Wszystkie dane, których właścicielem jest Wojskowa Akademia Techniczna podlegają ochronie w zakresie poufności, integralności i dostępności.
- 2. Wojskowa Akademia Techniczna jako administrator danych może udostępniać dane osobowe przetwarzane we własnych zbiorach:
 - 1) osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa;
 - 2) innym osobom i podmiotom w przypadku posiadania przez nich legalnych podstaw przetwarzania danych wynikających z przepisów o ochronie danych osobowych.

3. Udostępnianie danych nie może naruszać praw i wolności osób, których dane dotyczą i odbywa się na zasadach określonych w przepisach regulujących ochronę danych osobowych.
4. Dane osobowe mogą być udostępniane w następujących przypadkach:
 - 1) na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów;
 - 2) na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych;
 - 3) na podstawie wniosku osoby, której dane dotyczą.
5. Wniosek o udostępnienie danych osobowych powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie. Wzór wniosku stanowi Formularz nr 3 Polityki.
6. Udostępniając dane osobowe, należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
7. Kierownik jednostki organizacyjnej informuje IOD o otrzymanym wniosku udostępnienia danych osobowych od innego podmiotu niż wymieniony w ust. 2.
8. IOD przekazuje kierownikowi jednostki organizacyjnej opinię w sprawie udostępnienia danych.
9. Specjalista ds. ochrony danych jest odpowiedzialny za przygotowanie danych osobowych do udostępnienia w zakresie wskazanym we wniosku oraz udzielenia przedmiotowej odpowiedzi.
10. Osoba udostępniająca informacje dotyczące danych osobowych jest zobowiązana żądać pokwitowania pobrania dokumentów lub potwierdzenia wglądu w ich treść. Jeśli jednak pokwitowanie nie jest możliwe, osoba udostępniająca informację sporządza na tę okoliczność notatkę służbową.
11. Wniosek o udostępnienie danych osobowych, którego sposób rozpatrzenia budzi uzasadnione wątpliwości należy przesłać, wraz z informacjami niezbędnymi dla jego rozpatrzenia, do Sekcji Obsługi Prawnej w celu wydania opinii prawnej.
12. Specjalista ds. ochrony danych/LABI prowadzi rejestr udostępnienia danych.
13. IOD prowadzi rejestr udostępnienia danych na podstawie informacji uzyskanych od specjalisty ds. ochrony danych.
14. System informatyczny, w którym przetwarzane są dane podlegające udostępnieniu (gdy ma to zastosowanie) powinien umożliwiać odnotowanie: imienia i nazwiska osoby, która udostępnia dane osobowe, zakres udostępnionych danych i datę udostępnienia. Odnotowanie wyżej wymienionych informacji powinno nastąpić niezwłocznie po udostępnieniu danych.
15. Wojskowa Akademia Techniczna może odmówić udostępnienia danych osobowych. Odmowa udostępnienia danych osobowych następuje wówczas, gdy spowodowałoby to istotne naruszenia przepisów prawa, a w szczególności dóbr osobistych osób, których dane dotyczą, lub innych osób oraz jeżeli dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania wnioskodawcy.

16. Przekazanie danych na zewnątrz w formie elektronicznej powinno odbywać się przy użyciu środków zapewniających poufność i integralność informacji adekwatne do wagi przekazywanych danych.
17. Przekazywanie informacji do wiadomości publicznej odbywa się na podstawie *ustawy z dnia 6 września 2001 r., o dostępie do informacji publicznej* (Dz. U. z 2016 r., poz. 1764, z późn. zm).

Rozdział VIII

Prawa osób, których dane dotyczą

§ 23

1. Osoby, których dane są przetwarzane w WAT, mają prawo (na warunkach określonych w RODO) do: ochrony danych ich dotyczących, dostępu do treści swoich danych, ich sprostowania, usunięcia, ograniczenia przetwarzania, przenoszenia danych, wniesienia sprzeciwu, cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem, jak również do uzyskiwania wszystkich informacji o przysługujących im prawach.
2. Administrator danych w celu wypełnienia obowiązku informacyjnego wobec osób, których dane osobowe są przetwarzane w Wojskowej Akademii Technicznej, jest zobligowany do podania osobie której dane dotyczą wszystkich informacji wskazanych w RODO (tak zwana klauzula informacyjna). Wzór klauzuli informacyjnej określa Formularz nr 1 Polityki.

Rozdział IX

Upoważnienia do przetwarzania danych osobowych

§ 24

1. Do przetwarzania danych osobowych mogą być dopuszczone osoby, które spełniają łącznie następujące warunki:
 - 1) realizują zadania wymagające przetwarzania danych osobowych;
 - 2) odbyły szkolenie z zakresu ochrony danych osobowych;
 - 3) posiadają upoważnienie do przetwarzania danych osobowych.
2. Do przetwarzania danych osobowych uprawnione są tylko osoby upoważnione przez administratora danych.
3. Upoważnienie do przetwarzania danych osobowych wydaje AD lub specjalista ds. ochrony danych na wniosek kierownika jednostki organizacyjnej lub (jeśli ma to zastosowanie) specjalisty ds. ochrony danych według Formularza nr 6 Polityki. Wzór wniosku o nadanie/zmianę upoważnienia do przetwarzania danych osobowych określa Formularz nr 5 Polityki.
4. Upoważnienie do przetwarzania danych osobowych traci ważność w przypadku:
 - 1) zmiany przez osobę upoważnioną stanowiska lub jednostki organizacyjnej, w której jest zatrudniona lub pełni służbę;
 - 2) zmiany zakresu obowiązków, w wyniku której ustała konieczność przetwarzania danych osobowych;
 - 3) zawieszenia osoby w czynnościach służbowych;

- 4) zwolnienia osoby ze służby, pracy lub zakończenia współpracy z WAT na podstawie umowy, porozumienia;
- 5) cofnięcia upoważnienia lub upływu czasu, na który upoważnienie zostało udzielone.
5. Osoby, które zostały upoważnione do przetwarzania danych osobowych, składają oświadczenie o zapoznaniu się z przepisami i zasadami przetwarzania i ochrony danych osobowych. Wzór oświadczenia określa Formularz nr 7 Polityki.
6. Specjalista ds. ochrony danych/LABI przekazuje oświadczenie odpowiednio do Działu Personalnego lub Wydziału Kadr Wojskowych celem dołączenia do akt personalnych (kopia przeznaczona jest dla LABI).
7. Upoważnione osoby do przetwarzania danych osobowych są zobowiązane:
 - 1) nie ujawniać nikomu w żaden sposób i nie wykorzystywać informacji związanych z przetwarzanymi danymi osobowymi, z którymi zapoznali się w związku z wykonywaną pracą oraz zachować w tajemnicy także po ustaniu stosunku służby lub pracy, odwołaniu z pełnionej funkcji, zrealizowaniu umowy lub porozumienia;
 - 2) nie ujawniać sposobów ich zabezpieczenia przez cały czas realizacji zadań, a także po ustaniu stosunku służby lub pracy, odwołaniu z pełnionej funkcji, zrealizowaniu umowy lub porozumienia;
 - 3) zabezpieczać dane osobowe przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę postronną, zmianą, utratą, uszkodzeniem lub zniszczeniem.
8. Naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być uznane jako ciężkie naruszenie obowiązków pracowniczych i skutkować rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie przepisów *ustawy z dnia 26 czerwca 1974 r., Kodeks Pracy* (Dz. U. z 2018 r., poz. 108 z późn. zm).
9. Specjalista ds. ochrony danych odpowiada za dopuszczenie do przetwarzania danych osobowych wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych.
10. Ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzi specjalista ds. ochrony danych lub powołany przez niego LABI.
11. Cofnięcie upoważnienia do przetwarzania danych osobowych następuje z przyczyn, o których mowa w ust. 4 oraz może mieć miejsce w przypadkach, gdy:
 - 1) osoba spowodowała swoim celowym działaniem incydent mający negatywny wpływ na bezpieczeństwo przetwarzanych danych osobowych;
 - 2) istnieje uzasadniona obawa, podejrzenie, że przetwarzanie danych osobowych przez osobę wiąże się z poważnym ryzykiem utraty poufności, integralności lub dostępności tych danych.
12. Dane osobowe przechowuje się w sposób uniemożliwiający dostęp do nich osobom nieupoważnionych, realizując zasady ochrony, zabezpieczenia i kontroli przetwarzania przed dostępem do nich osób nieupoważnionych.
13. Osoby przetwarzające dane osobowe zobowiązane są w szczególności do:

- 1) ścisłego przestrzegania zakresu nadanego upoważnienia do przetwarzania danych osobowych;
- 2) przetwarzania i ochrony danych osobowych zgodnie z przepisami;
- 3) zachowania w tajemnicy loginów i haseł uwierzytelniających użytkownika w systemie do przetwarzania danych osobowych;
- 4) zachowania w tajemnicy informacji dotyczących przetwarzanych danych osobowych oraz sposobów i miejsc ich przechowywania i zabezpieczenia;
- 5) zgłaszania incydentów związanych z naruszeniem bezpieczeństwa ochrony danych osobowych oraz niewłaściwym funkcjonowaniem systemu przetwarzania danych.

Rozdział X

Szkolenia w zakresie zasad ochrony danych osobowych

§ 25

1. WAT realizując Politykę bezpieczeństwa danych osobowych zapewnia zaznajomienie osób upoważnionych do dostępu i przetwarzania danych osobowych z obowiązującymi przepisami prawa z zakresu ochrony danych osobowych, uregulowaniami wewnętrznymi, a także stosowanymi technikami i środkami ochrony tych danych w WAT.
2. Kierownik jednostki/komórki organizacyjnej powiadamia drogą elektroniczną IOD o potrzebie zapoznania z przepisami o ochronie danych osobowych nowo zatrudnioną osobę lub osobę rozpoczynającą współpracę na podstawie umowy, porozumienia.
3. Osoby, o których mowa w ust. 2 zaznajamiane są z zasadami ochrony danych osobowych przed dopuszczeniem do pracy lub wykonywania zadań na stanowiskach związanych z przetwarzaniem danych osobowych, a także odpowiednio, w trakcie trwania zatrudnienia lub trwania umowy – w przypadku zmian w obowiązujących przepisach prawa, uregulowaniach wewnętrznych lub stosowanych technikach i środkach ochrony danych w WAT.
4. Zapoznanie osób upoważnionych do przetwarzania danych osobowych z powszechnie obowiązującymi przepisami prawa, uregulowaniami wewnętrznymi, a także technikami i środkami ochrony tych danych, odbywa się w szczególności poprzez:
 - 1) instruktaż na stanowisku pracy;
 - 2) szkolenie wewnętrzne realizowane na terenie WAT (może odbywać się w oparciu o system e-learningu, generujący automatycznie zaświadczenie, po zaliczeniu z wynikiem pozytywnym testu wiedzy oraz tworzący wykaz przeszkolonych);
 - 3) szkolenie zewnętrzne.
5. W przypadku dostępu do danych osobowych przetwarzanych w systemie informatycznym, podstawowe szkolenie w zakresie procedur rozpoczęcia, zawieszenia i zakończenia pracy w systemie oraz mechanizmów zabezpieczenia stanowiska roboczego przeprowadza ASI.
6. Osoby przetwarzające dane osobowe zostają zaznajomione z zakresem informacji objętych tajemnicą w związku z wykonywanymi przez siebie zadaniami.

W szczególności są one informowane o powinności zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia.

7. Inspektor ochrony danych zobowiązany jest do zapoznawania osób zatrudnionych przy przetwarzaniu danych osobowych z obowiązującymi przepisami w tym zakresie i wydawania zaświadczeń o przeszkoleniu z obowiązującymi przepisami dotyczącymi ochrony danych osobowych. Wzór zaświadczenia stanowi Formularz nr 15 Polityki.
8. Zaświadczenie o przeszkoleniu wydaje się w dwóch egzemplarzach, jeden przeznaczony dla osoby upoważnionej, drugi do Działu Personalnego lub Wydziału Kadr Wojskowych celem dołączenia do akt personalnych.
9. IOD może w każdym czasie podjąć decyzję o sprawdzeniu wiedzy osób poddanych szkoleniu.
10. Osoby nieposiadające wiedzy z zakresu ochrony danych osobowych nie mogą być upoważnione do przetwarzania danych osobowych w WAT.
11. Na prośbę kierownika jednostki organizacyjnej, IOD może przeprowadzić szkolenie z ochrony danych osobowych w jednostce organizacyjnej.

Rozdział XI

Obszar przetwarzania danych osobowych

§ 26

1. Obszar, kompleks budynków, budynek, jedno lub kilka pomieszczeń zarówno na terenie chronionym jak i ogólnie dostępnym, w których przetwarzane są dane osobowe tworzą tzw. „obszar przetwarzania danych osobowych w WAT”.
2. Do obszaru przetwarzania danych osobowych w WAT, zalicza się również:
 - 1) pomieszczenia, w których są składowane uszkodzone nośniki komputerowe: taśmy, dyski, komputery, płyty CD, uszkodzone i przeznaczone do wycofania komputery i inne urządzenia z nośnikami zawierającymi dane osobowe;
 - 2) miejsca, w których wykonywana jest choćby jedna z czynności z zakresu przetwarzania danych.
3. Dane osobowe mogą być przetwarzane w budynkach i pomieszczeniach użytkowanych przez jednostki organizacyjne WAT, które są zlokalizowane wyłącznie w obrębie obszaru przetwarzania danych osobowych.
4. Dane osobowe mogą być przetwarzane w budynkach i pomieszczeniach podmiotów innych niż WAT, w których realizuje się zadania zgodnie z zawartymi z tymi podmiotami umowami, porozumieniami, gdy wynika to z charakteru realizowanych zadań.
5. Pomieszczenia tworzące obszar przetwarzania danych osobowych, na czas nieobecności upoważnionych pracowników powinny być zamykane w sposób uniemożliwiający dostęp osób postronnych. Zabrania się pozostawiania otwartych pomieszczeń podczas nieobecności pracowników.
6. Przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania dopuszczalne jest tylko w obecności upoważnionego pracownika.
7. Klucze oraz klucze zapasowe do pomieszczeń stanowiących obszar przetwarzania danych osobowych, przechowywane są (jeżeli ma to zastosowanie)

w portierni budynku, a także w elektronicznym systemie obiegu kluczy. Klucze dostępu muszą być jednoznacznie i trwale oznaczone numerem pomieszczenia. Po zakończeniu pracy pracownicy zdają klucze na portierni oraz do elektronicznego systemu obiegu kluczy.

8. Klucze wydawane są tylko pracownikom upoważnionym do przebywania w obszarze przetwarzania danych lub posiadający zgodę na przebywanie w obszarze przetwarzania danych osobowych.
9. Na portierni prowadzony jest rejestr osób upoważnionych do pobierania kluczy.
10. Zabronione jest wykonywanie nieautoryzowanych kopii kluczy umożliwiających dostęp do obszarów przetwarzania danych osobowych.
11. Dostęp do obszarów przetwarzania danych osobowych możliwy jest także za pomocą kart stykowych zgodnie z przyjętą w jednostce organizacyjnej polityką kluczy dostępu do obszaru przetwarzania danych.
12. Stanowiska pracy w obszarach przetwarzania danych osobowych, powinny być zorganizowane w taki sposób, aby podczas przebywania w pomieszczeniach osób nieuprawnionych uniemożliwić im nieautoryzowany dostęp do informacji zawartych w dokumentach papierowych czy monitorach komputerowych.
13. Specjaliści ds. ochrony danych zobowiązani są do bieżącego:
 - 1) prowadzenia wykazu obszaru przetwarzania danych osobowych w WAT, w podległych im lub przez nich nadzorowanych jednostkach organizacyjnych;
 - 2) informowania IOD – w formie pisemnej – o miejscach i zmianach ich lokalizacji, w których przetwarzane są dane osobowe zgodnie z Formularzem nr 12 Polityki.

Rozdział XII

Wykaz systemów i programów informatycznych do przetwarzania danych

§ 27

Wykaz systemów i programów informatycznych stanowi Załącznik nr 2 do Polityki.

Rozdział XIII

Sposób przepływu danych

§ 28

1. Sposób przepływu danych wymaga przedstawienia współpracy między różnymi podmiotami odpowiedzialnymi za przetwarzanie danych osobowych i systemami informatycznymi oraz relacje jakie istnieją między danymi zgromadzonymi.
2. Sposób przepływu danych wymaga zamieszczenia informacji o danych, które przenoszone są między systemami w sposób manualny (przy wykorzystaniu zewnętrznych nośników danych) lub automatycznie/półautomatycznie (za pomocą teletransmisji, przy wykorzystaniu specjalnych funkcji eksportu/importu danych).
3. Sposób przepływu danych pomiędzy systemami opisuje Formularz nr 13 Polityki bezpieczeństwa danych osobowych. Ewidencję prowadzi specjalista ds. ochrony danych/LABI oraz IOD.

Rozdział XIV
**Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności,
integralności i dostępności przetwarzanych danych osobowych**

§ 29

1. Oceniając czy stopień bezpieczeństwa jest odpowiedni należy szacować ryzyko wiążące się z przetwarzaniem danych osobowych.
2. Zarządzanie bezpieczeństwem przetwarzanych danych osobowych jest procesem ciągłym, realizowanym przy współdziałaniu wszystkich uczestników tego procesu.
3. Wojskowa Akademia Techniczna wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku z uwzględnieniem stanu wiedzy technicznej, kosztu wdrożenia oraz charakteru, zakresu, celu i kontekstu przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.
4. Administrator danych w szczególności uwzględnia ryzyko wiążące się z przetwarzaniem danych wynikające z:
 - 1) przypadkowego lub niezgodnego z prawem zniszczenia,
 - 2) utraty, modyfikacji, nieuprawnionego ujawnienia danych,
 - 3) nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
5. W celu ochrony danych Wojskowa Akademia Techniczna stosuje środki techniczne i organizacyjne:
 - 1) wyznaczono inspektora ochrony danych nadzorującego przestrzeganie zasad ochrony przetwarzanych danych osobowych;
 - 2) została opracowana i wdrożona dokumentacja ochrony danych osobowych;
 - 3) do przetwarzania danych osobowych dopuszczane są wyłącznie osoby posiadające upoważnienie;
 - 4) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych;
 - 5) osoby upoważnione zostały zapoznane z przepisami regulującymi ochronę danych osobowych;
 - 6) wydruki i inne dokumenty, informatyczne nośniki danych, w tym kopie zapasowe zawierające dane osobowe przechowuje się w zamykanych na klucz szafach, które znajdują się w budynkach i pomieszczeniach, w których przetwarzane są dane osobowe;
 - 7) zastosowane środki techniczne i organizacyjne w zależności od jednostki organizacyjnej Wojskowej Akademii Technicznej zostały oznaczone w rejestrze czynności przetwarzania danych osobowych;
 - 8) dla każdego systemu, w którym dokonuje się przetwarzania danych osobowych powołuje się administratora systemu informatycznego;
 - 9) administratora systemu informatycznego powołuje specjalista ds. ochrony danych dla każdego systemu informatycznego, zarządzanego przez kierowników podległych mu jednostek/komórek organizacyjnych;

- a) autonomicznego – przetwarzających dane osobowe na potrzeby podległej jednostki organizacyjnej;
 - b) o architekturze rozproszonej, rozległej, zarządzanego centralnie – zabezpieczającego przetwarzanie danych na potrzeby podległej i innych jednostek organizacyjnych WAT;
 - c) zewnętrznego, których użytkownikiem jest WAT.
6. Dla systemów o architekturze rozproszonej, zarządzanych centralnie, specjalista ds. ochrony danych może powołać lokalnego ASI. Celem jego działania jest (we współdziałaniu z ASI), koordynowanie wszelkich spraw związanych z funkcjonowaniem tych systemów w obszarze przetwarzania danych osobowych podległym specjaliście ds. ochrony danych.
 7. Szczegółowe zakresy działania ASI określa specjalista ds. ochrony danych.
 8. Kopię dokumentu powołania ASI należy przekazać odpowiednio do Działu Personalnego lub Wydziału Kadr Wojskowych celem dołączenia go do akt personalnych.
 9. Przetwarzanie danych osobowych powinno się odbywać z zastosowaniem ww. środków ochrony i w warunkach zabezpieczających te dane przed osobami nieupoważnionymi.
 10. W obszarze przetwarzania danych osobowych mogą przebywać osoby nieupoważnione tylko w obecności osoby upoważnionej do przetwarzania danych osobowych.
 11. Pracownicy przetwarzający dane osobowe obowiązani są do prawidłowego zabezpieczenia urządzeń i danych osobowych.
 12. Kierownicy jednostek organizacyjnych w porozumieniu z IOD zobowiązani są do wbudowania zasad ochrony prywatności w każdy projekt zakładający elementy ochrony danych osobowych tak, by od samego jego powstania ochrona prywatności stanowiła jego część składową (privacy by design). W celu zapewnienia możliwie jak najpełniejszego realizowania zasad ochrony danych, należy wykazać elementy planowania czynności np.:
 - 1) Minimalizacja danych – zaprojektowanie czynności, aby było możliwe jej wykonanie przy wykorzystaniu możliwie najmniejszej ilości środków;
 - 2) Pseudonimizacja – zaprojektowanie danej czynności tak, aby było możliwe jej wykonanie przy wykorzystaniu danych, których odczytanie nie jest możliwe bez klucza;
 - 3) Anonimizacja – polega na pozbawieniu danych osobowych i ich zbiorów cech pozwalających na identyfikację osób fizycznych, których dane dotyczą.
 13. W celu realizacji obowiązku wynikającego z art. 33 ust. 1 RODO WAT zobowiązana jest do zgłaszania naruszenia ochrony danych osobowych powodującego ryzyko naruszenia praw i wolności osób fizycznych do organu nadzorczego w czasie 72 godzin po stwierdzeniu naruszenia. Szczegóły określa Załącznik nr 1 do „*Polityki bezpieczeństwa danych osobowych w Wojskowej Akademii Technicznej*”).
 14. Przedstawiony katalog środków technicznych i organizacyjnych nie stanowi katalogu zamkniętego. Środki niezbędne dla zapewnienia poufności, integralności

i rozliczalności przetwarzania danych mogą zostać rozszerzone o środki zapewniające ochronę danych „dalej idącą”, to znaczy: zapewniające odpowiednie bezpieczeństwo danych osobowych.

Rozdział XV **Szacowanie i analiza ryzyka**

§ 30

1. Procedura ta ma miejsce przed rozpoczęciem przetwarzania danych osobowych w zbiorze celem oceny czy planowane przetwarzanie niesie za sobą wysokie ryzyko naruszenia praw lub wolności osób, których dane będą przetwarzane.
2. Jeżeli przetwarzanie danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, AD dokonuje oceny skutków planowanych operacji przetwarzania danych osobowych.
3. W przypadkach, gdy nie jest jasne, czy wymagane jest dokonanie oceny skutków dla ochrony danych, zaleca się jej wykonanie.
4. Ocena skutków dla ochrony danych osobowych nie jest wymagana, jeżeli przetwarzanie danych osobowych nie powoduje wysokiego ryzyka naruszenia ochrony danych osobowych.
5. Za przeprowadzenie oceny skutków dla ochrony danych odpowiedzialny jest specjalista ds. ochrony danych. Oceny merytorycznej co do konieczności przeprowadzenia oceny skutków dla ochrony danych przeprowadza się we współpracy z IOD.
6. Jeżeli ocena skutków dla ochrony danych wykaze, że przy braku zabezpieczeń, środków bezpieczeństwa oraz mechanizmów minimalizujących ryzyko przetwarzanie powodowałoby wysokie ryzyko naruszenia praw lub wolności osób fizycznych, a administrator wyraża opinię, że ryzyka tego nie da się zminimalizować środkami rozsądnymi z punktu widzenia dostępnych technologii i kosztów wdrożenia, wtedy przed rozpoczęciem czynności przetwarzania należy skonsultować się z organem nadzorczym.

Rozdział XVI **Zasady przetwarzania danych osobowych.**

§ 31

Dostęp do pomieszczeń, w których przetwarzane są dane osobowe

1. Zezwala się przetwarzać dane osobowe wyłącznie w budynkach i pomieszczeniach zlokalizowanych w granicach „obszaru przetwarzania danych osobowych WAT”.
2. Pomieszczenia i inne miejsca, w których są przetwarzane dane osobowe, powinny być chronione i zabezpieczone przed dostępem osób nieuprawnionych.
3. Wszystkie operacje na danych osobowych, mogą się odbywać wyłącznie w miejscach zabezpieczonych przed dostępem osób nieupoważnionych.
4. W pomieszczeniach, w których przetwarzane są dane osobowe mają prawo przebywać wyłącznie osoby upoważnione do ich przetwarzania oraz osoby sprawujące nadzór i kontrolę nad przestrzeganiem zasad przetwarzania i ochrony tych danych. Inne osoby wyłącznie w obecności upoważnionego

pracownika lub na podstawie upoważnienia wydanego przez specjalistę ds. ochrony danych lub inną upoważnioną osobę, według Formularza nr 8 Polityki.

5. Osoby nieposiadające upoważnienia do przetwarzania danych osobowych, a mające interes prawny lub faktyczny w uzyskaniu dostępu do danych oraz osoby wykonujące inne czynności niezwiązane z dostępem do danych osobowych, w szczególności takie, jak: sprzątanie, konserwacja, usuwanie awarii itp., mogą przebywać w pomieszczeniach i częściach pomieszczeń, w których przetwarzane są dane osobowe, wyłącznie za zgodą kierownika tej komórki organizacyjnej lub upoważnionej przez niego osoby i pod nadzorem upoważnionego pracownika. Na czas pobytu tych osób dokumenty i nośniki zawierające dane osobowe należy zabezpieczyć w sposób uniemożliwiający przypadkowe ich ujawnienie lub utracenie.
6. Stacje robocze systemu, powinny być umiejscowione w sposób uniemożliwiający osobom nieuprawnionym bezpośredni i niekontrolowany dostęp do ekranów oraz urządzeń końcowych oraz uniemożliwiać replikowanie danych.
7. W przypadku chwilowej nieobecności na stanowisku pracy należy zabezpieczyć stację roboczą przed możliwością jej użycia, np. przez zastosowanie wygaszaczy ekranu zabezpieczonych hasłem, a zbiory występujące w formach tradycyjnych zabezpieczyć przed dostępem osób nieuprawnionych. Opuszczenie miejsca pracy bez zabezpieczenia przed osobami postronnymi dostępu do danych osobowych, traktowane będzie jako naruszenie podstawowych obowiązków pracowniczych.
8. Klucze oraz kody dostępu do budynków i pomieszczeń oraz szaf i urządzeń do przechowywania nośników danych osobowych, powinny być przechowywane zgodnie z procedurą przewidzianą w „Planie ochrony WAT”, ewidencjonowane i wydawane osobom upoważnionym za pokwitowaniem.
9. W ewidencji uwzględnia się: imię i nazwisko osoby pobierającej lub zdającej klucz, numer lub inne oznaczenie pomieszczenia lub budynku oraz datę i godzinę pobrania lub zdanienia kluczy.
10. W przypadku, gdy w pomieszczeniu znajduje się część ogólnodostępna oraz część, w której przetwarzane są dane osobowe – część, w której są przetwarzane dane osobowe powinna być wyraźnie oddzielona od ogólnodostępnej. Wydzielenie części pomieszczenia, w której przetwarza się dane osobowe może być w szczególności realizowane poprzez montaż barierek, lad lub odpowiednie ustawienie mebli biurowych, uniemożliwiające lub co najmniej ograniczające niekontrolowany dostęp osób nieupoważnionych do danych osobowych przetwarzanych w danym pomieszczeniu.
11. Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych. Za proces tworzenia kopii zapasowych odpowiada ASI lub inna upoważniona przez ASI osoba.
12. Wydruki i inne dokumenty, informatyczne nośniki danych, w tym kopie zapasowe zawierające dane osobowe należy przechowywać w zamykanych na klucz szafach, które znajdują się w budynkach i pomieszczeniach, w których przetwarzane są dane osobowe. Klucze z szaf po zakończonej pracy są przechowywane w miejscu niedostępnym dla osób nieupoważnionych.

13. Niepotrzebne wydruki lub inne dokumenty należy niszczyć w niszczarkach o klasie niszczenia min. DIN 2, z uwzględnieniem przepisów dotyczących obiegu i archiwizacji dokumentów i innych nośników informacji w WAT.

§ 32

Zasady przetwarzania danych osobowych z wykorzystaniem systemów informatycznych

1. Za zabezpieczenie programowe systemu informatycznego odpowiada ASI, stosując wszelkie dostępne mu mechanizmy ochrony celem właściwego zabezpieczenia systemu do przetwarzania danych.
2. Każdy użytkownik posiadający upoważnienie do przetwarzania danych osobowych w systemie informatycznym otrzymuje od ASI, jednoznaczny i niepowtarzalny identyfikator do systemu oraz ustala hasło o odpowiedniej złożoności.
3. Sposób uwierzytelnienia użytkownika w systemie informatycznym określony został w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w WAT” stanowiącą Załącznik nr 2 do zarządzenia.
4. Jeżeli specyfika systemu informatycznego służącego do przetwarzania danych osobowych wymaga poszerzenia zasad zawartych w „Instrukcji”, ASI – w uzgodnieniu ze specjalistą ds. ochrony danych lub LABI – ma obowiązek pisemnego opracowania i wdrożenia uzupełniających procedur bezpieczeństwa dla tego systemu.
5. Systemy informatyczne służące do przetwarzania danych osobowych zabezpieczone są przed działaniami niepożądanymi na bieżąco aktualizowanymi systemami antywirusowymi przez ASI.
6. Dane osobowe przetwarzane są tylko w aplikacjach (programach) dostosowanych do merytorycznych potrzeb jednostek organizacyjnych WAT.
7. Przesyłanie danych pomiędzy systemami może odbywać się w sposób manualny, przy wykorzystaniu służbowych nośników zewnętrznych lub w sposób półautomatyczny albo automatyczny przy wykorzystaniu funkcji eksportu (importu) danych za pomocą teletransmisji w szczególności poprzez bezpieczną sieć komputerową.

§ 33

Zasady archiwizowania danych osobowych, niszczenia wydruków i zapisów na nośnikach magnetycznych

1. Kopie bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych wykonywane są zgodnie z zasadami określonymi w „Instrukcji zarządzania systemem”. Szczegółowe procedury tworzenia kopii bezpieczeństwa dla określonego systemu informatycznego służącego do przetwarzania danych w zależności od potrzeb, opracowuje ASI w uzgodnieniu ze specjalistą ds. ochrony danych.
2. Za prawidłowe wykonanie kopii bezpieczeństwa odpowiada właściwy ASI.
3. Sposób, miejsce i okres przechowywania i niszczenia nośników danych osobowych, w tym kopii bezpieczeństwa zawiera „Instrukcja zarządzania

systemem informatycznym służącym do przetwarzania danych osobowych w WAT”.

4. Uszkodzone nośniki danych osobowych (przeznaczone do wybrakowania) przed ich wycofaniem z użytkowania są fizycznie niszczone w sposób uniemożliwiający ich odczytanie.
5. Zabrania się przekazywania nośników danych na zewnątrz innym użytkownikom, na których uprzednio zapisane były dane osobowe.
6. Sposób postępowania z nośnikami danych osobowych określa *Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w WAT*.
7. Po wykorzystaniu dokumenty papierowe zawierające dane osobowe niepotrzebne w pracy bieżącej oraz niepodlegające archiwizacji, są niszczone w sposób uniemożliwiający ich odczytanie. Zabrania się przekazywania na makulaturę, dokumentów częściowo zniszczonych.
8. Niszczenie zbędnych danych osobowych i ich zbiorów w szczególności polega na:
 - 1) trwałym, fizycznym zniszczeniu danych osobowych i ich zbiorów wraz z ich nośnikami w stopniu uniemożliwiającym ich późniejsze odtworzenie przy stosowaniu powszechnie dostępnych metod;
 - 2) anonimizacji danych osobowych i ich zbiorów polegającej na pozbawieniu danych osobowych i ich zbiorów cech pozwalających na identyfikację osób fizycznych, których dane dotyczą.
9. Osoby przetwarzające dane osobowe w WAT mają obowiązek stosowania oddanych im do dyspozycji narzędzi i technik niszczenia zbędnych danych osobowych lub ich zbiorów.
10. Naruszanie zasad niszczenia zbędnych danych osobowych lub ich zbiorów, traktowane będzie jako ciężkie naruszenie podstawowych obowiązków pracowniczych ze wszystkimi wynikającymi stąd konsekwencjami, z rozwiązaniem stosunku pracy włącznie.

§ 34

Zasady zapewniania ciągłości działania systemów

1. Kluczowe urządzenia systemów informatycznych podłączone są do urządzeń podtrzymujących napięcie (UPS), w celu umożliwienia bezpiecznego wyłączenia systemu w przypadku awarii zasilania.
2. W przypadku awarii systemu informatycznego lub jego elementów, ASI przy współudziale kierownika jednostki organizacyjnej odpowiedzialnego za zarządzanie systemem, niezwłocznie podejmuje niezbędne działania minimalizujące skutki awarii.
3. Naprawa, serwisowanie urządzeń i sprzętu związanego z bezpieczeństwem przetwarzania informacji powinno następować w możliwie krótkim czasie od wykrycia jego awarii. Szybkie przywrócenie właściwego stanu technicznego urządzeń ma na celu wyeliminowanie z użycia sprzętu, który nie spełnia wymaganych parametrów zapewniających bezpieczeństwa przetwarzanych

danych. Nie jest dopuszczalne rezygnowanie z zabezpieczeń z powodu ich wadliwego działania spowodowanego awarią.

Rozdział XVII

Przekazywanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej

§ 35

1. Przekazywanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić tylko, gdy spełnione zostaną warunki i unormowania wynikające z RODO przy zapewnieniu, że nie został naruszony stopień ochrony osób fizycznych wyrażony w RODO.
2. Podstawowym warunkiem przekazania danych osobowych do państwa trzeciego jest stwierdzenie przez Komisję Europejską, że państwo trzecie lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony danych osobowych. Stwierdzenie odpowiedniego stopnia ochrony następuje w postaci aktu wykonawczego zawierającego decyzję Komisji Europejskiej.
3. Przekazanie danych osobowych do państw trzecich lub organizacji międzynarodowych w odniesieniu, do których podjęta została decyzja o zapewnieniu odpowiedniego stopnia ochrony danych nie wymaga specjalnego zezwolenia.
4. W przypadku konieczności przekazywania danych osobowych do państwa trzeciego, przekazanie to następuje zgodnie z Rozdziałem V art. 44 – 49 RODO.

Rozdział XVIII

Naruszenie zasad ochrony danych osobowych

§ 36

1. Wszystkie osoby przetwarzające dane osobowe w WAT mają obowiązek informowania swojego przełożonego o zauważonych incydentach naruszenia bezpieczeństwa.
2. Wystąpienie incydentu jest każdorazowo analizowane przez IOD, specjalistę ds. ochrony danych/LABI i ASI w celu wprowadzenia zmian i usprawnień w systemie bezpieczeństwa informacji.
3. Specjalista ds. ochrony danych/LABI i ASI w porozumieniu z IOD organizują działania mające na celu minimalizację ryzyka wystąpienia zagrożeń poprzez planowanie i wdrażanie nowych zabezpieczeń, procedur, rozwiązań oraz analizę wykrytych incydentów.
4. ASI stale monitorują poziom bezpieczeństwa oraz pojawiające się zagrożenia administrowanych systemów informatycznych.
5. Każda osoba, która stwierdziła:
 - 1) zgubienie lub kradzież komputera przenośnego, pamięci zewnętrznej, telefonu służbowego bądź innego nośnika zawierającego dane osobowe;
 - 2) naruszenie bezpieczeństwa systemu informatycznego;
 - 3) naruszenie technicznego stanu urządzeń służących do przetwarzania danych osobowych;
 - 4) naruszenie zawartości zbioru danych osobowych;

- 5) ujawnienie metod pracy lub sposobów działania programu osobom trzecim;
- 6) zmianę jakości transmisji danych w sieci telekomunikacyjnej mogącą wskazywać na naruszenie zabezpieczenia tych danych;
- 7) zaistnienie zdarzeń mogących mieć wpływ na naruszenie bezpieczeństwa danych osobowych;

zobowiązana jest niezwłocznie powiadomić o tym fakcie bezpośredniego przełożonego, specjalistę ds. ochrony danych/LABI oraz IOD.

6. Szczegółowe zasady postępowania w przypadku odnotowania incydentu w ochronie danych osobowych zamieszczono w instrukcji postępowania w sytuacjach naruszenia zasad ochrony danych osobowych stanowiącej Załącznik nr 1 do Polityki bezpieczeństwa.

Rozdział XIX **Odpowiedzialność**

§ 37

Pracownik, który przetwarza dane osobowe w WAT w sposób niezgodny z prawem podlega odpowiedzialności określonej w przepisach odrębnych.

Rozdział XX **Postanowienia końcowe**

§ 38

1. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy *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)*, inne przepisy Unii Europejskiej, prawa krajowego oraz wewnętrzne akty prawne regulujących ochronę danych osobowych.
2. Wszystkie osoby przetwarzające dane osobowe w WAT zobowiązane są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w „*Polityki bezpieczeństwa przetwarzania danych osobowych w Wojskowej Akademii Technicznej*”.

Klauzula informacyjna (wzór)

Zgodnie z art. 13 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), informuję, iż:

1. Administratorem Pani/Pana danych osobowych jest Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego z siedzibą w Warszawie (kod: 00-908) przy ul. Gen. Witolda Urbanowicza 2;
2. Administrator danych powołał inspektora ochrony danych nadzorującego prawidłowość przetwarzania danych osobowych, z którym można się skontaktować za pośrednictwem adresu e-mail: iod@wat.edu.pl
3. Pani/Pana dane osobowe będą przetwarzane w celu: [należy wskazać wszystkie cele przetwarzania danych];
4. Podane dane będą przetwarzane na podstawie [należy wskazać podstawę prawną wynikającą z art. 6 ust. 1 ogólnego rozporządzenia o ochronie danych osobowych];
5. Podanie danych jest dobrowolne [jeżeli podanie danych jest obowiązkiem należy wskazać podstawę prawną – np. przepis ustawy], jednak konieczne do realizacji celów do jakich zostały zebrane;
6. Dane osobowe nie będą udostępniane innym odbiorcom, z wyjątkiem przypadków przewidzianych przepisami prawa [jeżeli dane będą przekazywane innym podmiotom np. ZUS, MNiSW, lub na podstawie umowy powierzenia należy wskazać te podmioty];
7. Dane przechowywane będą przez okres [np. cel archiwizacyjny – dane studentów – 50 lat, do odwołania zgody, konkretny termin itp.];
8. Posiada Pani/Pan prawo dostępu do treści swoich danych oraz z zastrzeżeniem przepisów prawa: prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo do wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
9. Ma Pani/Pan prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych;
10. Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany i nie będą poddawane profilowaniu.

Potwierdzam, że zapoznałem(am) się i przyjmuję do wiadomości powyższe informacje.

.....
Miejscowość, data, czytelny podpis

Klauzula zgody (wzór)

Wyrażam zgodę na przetwarzanie moich danych osobowych przez Wojskową Akademię Techniczną im. Jarosława Dąbrowskiego z siedzibą w Warszawie (kod: 00-908) przy ul. Gen. Witolda Urbanowicza 2 w celu:

☐.....;

☐.....;

☐.....

zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 oraz ustawą o ochronie danych osobowych z dnia
(Dz.U.....) oraz zgodnie z klauzulą informacyjną dołączoną do mojej zgody.

.....
Miejscowość, data, czytelny podpis

WNIOSEK O UDOSTĘPNIENIE DANYCH OSOBOWYCH

1. Wniosek do:

.....

(dokładna nazwa administratora danych)

2. Wnioskodawca

.....

(imię i nazwisko/nazwa firmy/dane do korespondencji)

3. Podstawa prawna upoważniająca wnioskodawcę do przetwarzania danych osobowych jako odbiorcy danych:

1)

2)

4. Cel przetwarzania danych:

1)

2)

5. Nazwa zbioru danych, z którego mają być udostępnione dane osobowe, lub informacje umożliwiające zidentyfikowanie dokumentów, w których występowały dane osobowe:

1)

2)

6. Zakres wymaganych danych, jakie mają być udostępnione:

1)

2)

7. Forma doręczenia udostępnianych danych osobowych:

.....

8. Oświadczam, że jestem osobą upoważnioną do uzyskania żądania we wniosku odpowiedzi.

Data i podpis osoby wnioskującej

REJESTR UDOSTĘPNIONYCH DANYCH

Lp.	Numer wniosku	Data udostępnienia danych	Nazwa podmiotu/wnioskodawcy któremu udostępniono dane	Podstawa prawna udostępnienia danych	Zakres udostępnionych danych	Imię i nazwisko osoby udostępniającej dane
1.						
2.						
3.						
4.						

*Data i podpis specjalisty
ds. ochrony danych*

WNIOSEK O WYDANIE / MODYFIKACJĘ / UNIEWAŻNIENIE UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

(imię i nazwisko/stanowisko/funkcja)

(nazwa jednostki organizacyjnej)

Wniosek obejmuje dostęp do danych przetwarzanych w Wojskowej Akademii Technicznej
W [należy wskazać jednostkę organizacyjną/komisję rekrutacyjną/stypendialną/konkursową/inne]:

- ☐
- ☐
- ☐
- ☐

Miejsce przetwarzania danych.....

Kategoria danych osobowych *:

- ☐ dane kandydatów do pracy: TAK/NIE,
- ☐ dane pracownicze kadrowe: TAK/NIE,
- ☐ dane pracownicze płacowe: TAK/NIE,
- ☐ dane pracownicze socjalne: TAK/NIE,
- ☐ dane studenckie: TAK/NIE,
- ☐ dane doktorantów: TAK/NIE,
- ☐ dane kandydatów na studia: TAK/NIE,
- ☐ dane absolwentów: TAK/NIE,
- ☐ dane czytelników bibliotek: TAK/NIE,
- ☐ inne [wymienić jakie]:

Operacja na danych osobowych*:

- ☐ przeglądanie: TAK/NIE,
- ☐ modyfikacja: TAK/NIE,
- ☐ usuwanie: TAK/NIE,
- ☐ zbieranie: TAK/NIE,
- ☐ udostępnianie: TAK/NIE,
- ☐ wprowadzanie: TAK/NIE,
- ☐ przechowywanie: TAK/NIE,
- ☐ weryfikacja: TAK/NIE,
- ☐ archiwizowanie: TAK/NIE,
- ☐ inne [wymienić jakie]:

Forma przetwarzania danych osobowych*:

- ☐ system/y informatyczny/e [wymienić jakie]:
- ☐ dane osobowe przetwarzane w wersji papierowej: TAK/NIE,
- ☐ inne [wymienić jakie]:

Okres obowiązywania:

na czas określony: od do,
na czas zgodny z zatrudnieniem*,
na czas pełnienia funkcji: od do

*Data i podpis kierownika
jednostki organizacyjnej*

*właściwe podkreślić

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH WOJSKOWEJ AKADEMII TECHNICZNEJ

Nr

Reprezentując Wojskową Akademię Techniczną im. Jarosława Dąbrowskiego, z siedzibą w Warszawie (kod: 00-908) przy ul. Gen. Witolda Urbanowicza 2, jako administrator danych upoważniam Panią/Pana:

(imię i nazwisko/stanowisko/funkcja)

(nazwa jednostki organizacyjnej)

do przetwarzania danych osobowych w Wojskowej Akademii Technicznej.

Niniejsze upoważnienie obejmuje dostęp do danych przetwarzanych w Wojskowej Akademii Technicznej w [należy wskazać jednostkę organizacyjną, /komisję rekrutacyjną/stypendialną/konkursową/inne]:

-
-
-
-

Rodzaj i zakres danych osobowych*:

- dane kandydatów do pracy: TAK/NIE,
- dane pracownicze kadrowe: TAK/NIE,
- dane pracownicze płacowe: TAK/NIE,
- dane pracownicze socjalne: TAK/NIE,
- dane studenckie: TAK/NIE,
- dane doktorantów: TAK/NIE,
- dane kandydatów na studia: TAK/NIE,
- dane absolwentów: TAK/NIE,
- dane czytelników bibliotek: TAK/NIE,
- inne [wymienić jakie]:

Forma przetwarzania danych osobowych*:

- z użyciem systemu informatycznego: TAK/NIE,
- dane osobowe przetwarzane w wersji papierowej: TAK/NIE,
- inne [wymienić jakie]:

Okres obowiązywania:

na czas określony: od do

na czas zgodny z zatrudnieniem*,

na czas pełnienia funkcji: od do

Upoważniony obowiązany jest do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz przepisami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (Dz. U. UE L 119 z 04.05.2016 r.), prawa krajowego oraz wewnętrznymi aktami prawnymi regulującymi ochronę danych osobowych.

Osoba upoważniona zobowiązana jest do nieujawniania, w żadnej postaci i treści, informacji dotyczących danych osobowych zawartych w zbiorach danych Wojskowej Akademii Technicznej, z wyjątkiem sytuacji, gdy jest to niezbędne dla celów służbowych, a także do postępowania z danymi, zgodnie z obowiązującymi regulacjami wewnątrzuczelnianymi, w szczególności zachowania ich poufności, integralności oraz właściwego ich zabezpieczenia.

Naruszenie obowiązków w zakresie ochrony danych osobowych, w szczególności ich udostępnianie lub umożliwienie dostępu osobie nieupoważnionej może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów prawa regulujących ochronę danych osobowych oraz stanowić ciężkie naruszenie obowiązków pracowniczych.

Data i podpis osoby
upoważnionej

Data i podpis specjalisty
ds. ochrony danych

Identyfikator osoby upoważnionej:

.....
(Nazwisko ASI, data)

*właściwe podkreślić

.....
(imię i nazwisko pracownika)

.....
(stanowisko służbowe)

.....
(nazwa jednostki organizacyjnej)

**Oświadczenie
pracownika/ żołnierza zawodowego o zapoznaniu się z przepisami
z zakresu ochrony informacji i danych osobowych
w Wojskowej Akademii Technicznej**

Oświadczam, iż w związku z realizacją zleconych mi czynności i zadań zastałam/em zapoznany z przepisami z zakresu ochrony danych osobowych, w szczególności z Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 oraz ustawy o ochronie danych osobowych z dnia (Dz.U.....) i przepisów wykonawczych do niej oraz aktów prawnych wewnętrznych obowiązujących w Akademii dotyczących przetwarzania danych osobowych.

W związku z powyższym oświadczam, że znane są mi przepisy dotyczące ochrony i zapewnienia bezpieczeństwa przetwarzania danych osobowych oraz obowiązki spoczywające na osobach mających dostęp do przedmiotowych danych i zobowiązuję się do ich przestrzegania, przetwarzania zgodnie z udzielonym mi upoważnieniem, ochrony danych przed niepożądanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem, wykorzystywania wyłącznie do celów służbowych, zarówno w trakcie trwania jak i po ustaniu zatrudnienia/ służby zawodowej w WAT, pod rygorem odpowiedzialności z tytułu naruszenia obowiązujących przepisów i aktów prawnych wewnętrznych.

Zostałem również poinformowany o nadzorze i kontroli pracodawcy nad prawidłowością postępowania w zakresie bezpieczeństwa informacji i danych osobowych przetwarzanych w postaci tradycyjnej oraz w systemach informatycznych, w szczególności w udostępnionych mi do wykorzystania urządzeniach i aplikacjach.

.....
(miejscowość, data)

.....
(czytelny podpis pracownika/żołnierza)

ZGODA NR.....

NA PRZEBYWANIE W OBSZARZE PRZETWARZANIA DANYCH OSOBOWYCH

Reprezentując Wojskową Akademię Techniczną im. Jarosława Dąbrowskiego, z siedzibą w Warszawie (kod: 00-908) przy ul. Gen. Witolda Urbanowicza 2, jako administrator danych / w imieniu administratora danych * upoważniam Panią/Pana*:

Imię i nazwisko

Nazwa jednostki organizacyjnej

na przebywanie w obszarze przetwarzania danych osobowych w zakresie niezbędnym do wykonywania:

☐ obowiązków służbowych,

☐ prac zleconych,

☐ innych zadań tj.:

Zgoda jest ważna do dnia: / do odwołania.

Data i podpis specjalisty

ds. ochrony danych

OŚWIADCZENIE

W związku z udzieleniem mi zgody na przebywanie w obszarze przetwarzania danych osobowych zobowiązuję się do zachowania w tajemnicy informacji pozyskanych w trakcie realizacji obowiązków, w tym danych osobowych oraz informacji o sposobie ich przechowywania i zabezpieczania. Jednocześnie zobowiązuję się wykonywać swoje obowiązki nie naruszając przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (Dz. U. UE L 119 z 04.05.2016 r.), prawa krajowego oraz wewnętrznych aktów prawnych regulujących ochronę danych osobowych.

Data i podpis osoby,

której udzielono zgody

*właściwe podkreślić

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH
(SPECJALISTA DS. OCHRONY DANYCH)

Lp.	Czynność przetwarzania danych osobowych	Cel przetwarzania danych osobowych	Podstawa prawna przetwarzania danych osobowych	Opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych	Zakres danych osobowych	Sposób zbierania danych osobowych	Fizyczna lokalizacja przetwarzania danych osobowych	Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych	Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazania, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń	Planowany termin usunięcia poszczególnych kategorii danych	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO	Dane podmiotu, któremu powierzono przetwarzanie danych
1	2	3	4	5	6	7	8	9	10	11	12	13
1												
2												

.....
Sporządził, nazwisko i imię, podpis

.....
Nazwisko, data i podpis specjalisty ds. ochrony danych

**REJESTR WSZYSTKICH KATEGORII CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH
DOKONYWANYCH W IMIENIU ADMINISTRATORA
(SPECJALISTA DS. OCHRONY DANYCH)**

Lp.	Imię i nazwisko lub nazwa oraz dane kontaktowe administratora danych w imieniu którego działa WAT, (a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego)	Dane kontaktowe inspektora ochrony danych	Kategorie przetwarzania dokonywanych w imieniu administratora	Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazania, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO	Data, numer umowy głównej/ o powierzeniu danych osobowych (jeżeli podpisano) wraz z datami ich podpisania	Czas trwania umowy	Zasady zakończenia współpracy (np. zniszczenie danych, oddanie danych)
1	2	3	4	5	6	7	8	9
1								
2								
3								

.....
Sporządził, nazwisko i imię, podpis

.....
Nazwisko, data i podpis specjalisty ds. ochrony danych

nazwa jednostki organizacyjnej

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Imię i nazwisko użytkownika	Nr wydanego upoważnienia	Nr identyfikatora w systemie informatycznym	Data wydania upoważnienia	Data cofnięcia upoważnienia	Czas obowiązywania	Forma przetwarzania danych
1.							
2.							
3.							

.....
Nazwisko, data i podpis specjalisty ds. ochrony danych

nazwa jednostki organizacyjnej

WYKAZ OBSZARÓW PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Nazwa procesu /czynności przetwarzania danych	Lokalizacja	Środki ochrony fizycznej danych	Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej	Środki ochrony w ramach narzędzi programowych i baz danych	Środki organizacyjne
1.	<i>podać nazwę procesu/czynności przetwarzania danych</i>	<i>podać adres budynku, nazwę pomieszczenia lub części pomieszczenia</i>	<i>podać skrót zabezpieczenia z legendy</i>	<i>podać skrót zabezpieczenia z legendy</i>	<i>podać skrót zabezpieczenia z legendy</i>	<i>podać skrót zabezpieczenia z legendy</i>
2.						
3.						

.....
Sporządził, nazwisko i imię, podpis

.....
Nazwisko, data i podpis specjalisty ds. ochrony danych

Skróty oznaczenia środków ochrony fizycznej danych:

DZ	– drzwi zwykłe (niewzmacniane, nie przeciwpożarowe)
DO	– drzwi o podwyższonej odporności ogniowej ≥ 30 min.
DW	– drzwi o podwyższonej odporności na włamanie – drzwi klasy C
KR	– okna zabezpieczone za pomocą krat, rolet lub folii antywłamaniowej
SA	– system alarmowy przeciwwłamaniowy
SK	– system kontroli dostępu
SM	– system monitoringu z zastosowaniem kamer przemysłowych
SO	– obszar nadzorowany przez służbę ochrony (całodobowo)
ZS	– zamknięta na klucz niemetalowa szafa
ZM	– zamknięta na klucz metalowa szafa
KP	– zamknięty sejf lub kasa pancerna
KZS	– kopia zapasowa przechowywana w zamkniętej na klucz niemetalowej szafie
KZM	– kopia zapasowa przechowywana w zamkniętej na klucz metalowej szafie
KZP	– kopia zapasowa przechowywana w zamkniętym sejfie lub kasie pancerniej
KT	– dane przechowywane w kancelarii tajnej
PPOŻ	– system przeciwpożarowy i/lub wolno stojąca gaśnica

Skróty oznaczenia środków sprzętowych infrastruktury informatycznej i telekomunikacyjnej:

SL	– komputery połączone z lokalną siecią komputerową
UPS	– zastosowano UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną
BIOS	– zastosowano hasło BIOS
IH	– zastosowano identyfikator użytkownika oraz hasło
TOK	– zastosowano karty procesorowe oraz kod PIN lub token
BIO	– zastosowano uwierzytelnianie biometryczne
AUT	– zastosowano środki uniemożliwiające wykonanie nieautoryzowanej kopii
HZ	– zastosowano systemowe mechanizmy wymuszające okresową zmianę haseł
RD	– zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych
KRT	– zastosowano środki kryptograficznej ochrony danych w teletransmisji
UT	– zastosowano mechanizm uwierzytelniania przy dostępie do środków teletransmisji
CALL	– zastosowano procedurę oddzwaniania przy transmisji za pośrednictwem modemu
MD	– zastosowano macierz dyskową
ANW	– zastosowano program antywirusowy
FW	– zastosowano system Firewall przy dostępie do sieci komputerowej
IDS	– zastosowano system IDS/IPS

NIS – niszczarki do dokumentów

Inne

Skróty oznaczenia środków ochrony w ramach narzędzi programowych i baz danych:

REJ – zastosowano rejestrację zmian wykonywanych na poszczególnych elementach zbioru

DOS – określono prawa dostępu do wskazanego zakresu danych

PIH – zastosowano identyfikator użytkownika oraz hasła

PTOK – zastosowano karty procesorowe oraz kod PIN lub token

PBIO – zastosowano technologię biometryczną

PRD – zastosowano system rejestracji dostępu do systemu/zbioru danych os.

PZH – zastosowano okresową zmianę haseł dostępu

PKRY – zastosowano kryptograficzne środki ochrony danych

WYG – zainstalowano wygaszacze ekranów

BLOK – zastosowano automatyczną blokadę dostępu w przypadku dłuższej nieaktywności pracy użytkownika

Inne

Inne

Skróty oznaczenia środków organizacyjnych:

OU – osoby upoważnione zostały zaznajomione z przepisami o ochronie danych

SZ – osoby upoważnione zostały przeszkolone z zabezpieczeń systemu informatycznego

OP – osoby upoważnione zostały zobowiązane do zachowania danych w poufności

PE – zastosowano politykę czystego ekranu

KZ – kopia zapasowa danych jest przechowywana w innym pomieszczeniu niż oryginał

LABI – wyznaczono lokalnego administratora bezpieczeństwa informacji

ASI – wyznaczono administratora systemu informatycznego

EU – prowadzona ewidencja osób upoważnionych do przetwarzania danych osobowych

EP – prowadzona ewidencja osób przeszkolonych z danych osobowych

DD – wdrożono dokumentację ochrony danych osobowych

Inne

.....
nazwa jednostki organizacyjnej

OPIS PRZEPŁYWU DANYCH OSOBOWYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

System (Moduł) A	System (Moduł) B	Kierunek przepływu danych osobowych	Sposób przesyłania danych osobowych
<i>podać nazwę programu z którego przepływają dane osobowe</i>	<i>podać nazwę programu do którego są przesyłane dane osobowe</i>	<i>określić kierunek przepływu np. jednokierunkowo, dwukierunkowo lub wielokierunkowo</i>	<i>określić sposób przesyłania danych np. manualnie, automatycznie lub półautomatycznie</i>
Przykład			
System AAAAAA	ProgramBBBBBB	Jednokierunkowo z programu AAAA do programu bibliotecznego BBBB	Półautomatyczny eksport pliku z systemu AAAAAA do programu BBBB
Program płacowo-kadrowy KAD-PLA	Program płacowy XYXYE	Jednokierunkowo z programu kadrowo-płacowego KAD- PLA do programu XYXYE	Półautomatycznie – eksport z pliku kadrowo-płacowego KAD-PLA na serwer, który następnie pobierany jest przez program XYXYE
Program SOSYTOR	Program FORTUN	Dwukierunkowo, synchronizacja danych o studentach pomiędzy systemami	Automatycznie raz na dobę o godz. 16.00.
Program SOSYTOR	Program do RAPTOR	Jednokierunkowo z programu SOSYTOR do programu RAPTOR	Manualny eksport z systemu SOSYTOR na nośniku - do programu RAPTOR
Program SOSYTOR	Program PORYT	Jednokierunkowo z programu SOSYTOR do programu PORYT	Automatycznie jeden raz w ciągu doby o godz. 14.00

.....
Sporządził, nazwisko i imię, podpis

.....
Nazwisko imię, podpis specjalisty ds. ochrony danych

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Nr / r.

Zawarta w dniu r. w Warszawie pomiędzy:

Wojskową Akademią Techniczną im. Jarosława Dąbrowskiego z siedzibą w Warszawie 00-908 Warszawa 46, ul. Gen. Witolda Urbanowicza 2, NIP 527-020-63-00, Regon 012122900 zwaną w dalszej części niniejszej umowy „Administratorem”, reprezentowaną przez:

..... –

a

.....

.....

Zwaną/ym w dalszej części niniejszej umowy „Podmiotem przetwarzającym”, reprezentowaną/ym przez:

..... –

zwanymi dalej łącznie „Stronami”

o następującej treści:

§ 1**Powierzenie przetwarzania danych osobowych**

1. W związku z realizacją umowy nr z dnia r. pomiędzy a, w sprawie Administrator powierza Podmiotowi przetwarzającemu 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 „Rozporządzeniem”, przetwarzanie danych osobowych.
2. Administrator oświadcza, że w rozumieniu Rozporządzenia jest administratorem zbioru danych osobowych pod nazwą
3. Administrator powierza Podmiotowi przetwarzającemu dane osobowe z wyżej wymienionego zbioru, zwanego dalej „Dane” w zakresie określonym niniejszą umową i poleca Podmiotowi przetwarzającemu ich przetwarzanie.
4. Podmiot przetwarzający oświadcza, że profesjonalnie zajmuje się działalnością objętą zakresem niniejszej umowy oraz gwarantuje, że ma odpowiednią wiedzę, wiarygodność i zasoby dla jej realizacji.

§ 2

Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie niniejszej umowy Dane określone w postaci nazwy zbioru danych, rodzaju danych, tj. zwykłych, szczególnych zgodnie z kategoriami art. 9 Rozporządzenia, kategorie osób, których dane dotyczą (jak pracownik, student itp.), w postaci (imię, nazwisko, adres, PESEL, nr telefonu, itp.):
 - 1)
 - 2)
2. Powierzone przez Administratora Dane będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu wykonywania usług szczegółowo opisanych w umowie, o której mowa w § 1 ust. 1 i w sposób zgodny z niniejszą umową.
3. Dane będą przetwarzane przez Podmiot przetwarzający przy wykorzystaniu systemów informatycznych oraz w wersji tradycyjnej (papierowej), wyłącznie w celu prawidłowej realizacji przedmiotu umowy.
4. Podmiot przetwarzający uprawniony jest do wykonywania na Danych jedynie takich operacji, które są niezbędne do wykonywania przedmiotu umowy.

§ 3

Sposób wykonania umowy powierzenia w zakresie przetwarzania danych osobowych

1. Podmiot przetwarzający w każdym przypadku będzie dokonywał przetwarzania Danych wyłącznie zgodnie z przepisami prawa, niniejszą umową oraz dobrymi praktykami stosowanymi w dziedzinie ochrony danych osobowych. Strony przez przepisy prawa rozumieją wszelkie akty prawa krajowego i europejskiego obowiązujące Administratora, z uwzględnieniem ich ewentualnych zmian, które nastąpią w okresie obowiązywania niniejszej umowy, zwane dalej „Aktami Prawnymi”.
2. Podmiot przetwarzający oświadcza, iż prowadzi rejestr czynności przetwarzania oraz dysponuje odpowiednimi środkami, w tym należyтыми zabezpieczeniami umożliwiającymi przetwarzanie danych osobowych zgodnie z Rozporządzeniem. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych Danych, do ich zabezpieczenia poprzez podjęcie środków technicznych i organizacyjnych, o których mowa art. 32 Rozporządzenia, zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, 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. Do przetwarzania Danych Podmiot przetwarzający dopuści jedynie osoby, które:
 - 1) zostały przeszkolone przez Podmiot przetwarzający z tematyki ochrony danych osobowych;
 - 2) posiadają indywidualne upoważnienia do przetwarzania danych osobowych nadane przez Podmiot przetwarzający;
 - 3) zobowiązały się (w formie pisemnej) do przestrzegania zasad ochrony danych osobowych, w tym do zachowania poufności Danych, jak również sposobów ich zabezpieczania oraz oświadczyły, iż znają obowiązujące przepisy prawa.

4. Podmiot przetwarzający oświadcza, że każda osoba upoważniona do przetwarzania Danych jest zobowiązana do bezterminowego zachowania Danych w tajemnicy.

§ 4

Obowiązki Podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się do przetwarzania Danych wyłącznie w zakresie określonym niniejszą umową.
2. Przetwarzanie przez Podmiot przetwarzający Danych w zakresie oraz celach innych niż objęte upoważnieniem udzielonym w treści niniejszej umowy i wyraźnie wskazane w jej postanowieniach, jest niedopuszczalne.
3. Podmiot przetwarzający będzie prowadził ewidencję osób upoważnionych do przetwarzania Danych, w tym mających dostęp do systemów informatycznych, w których przetwarzane są Dane będące przedmiotem niniejszej umowy.
4. Podmiot przetwarzający zobowiązuje się nie ujawniać osobom nieupoważnionym informacji o Danych, zwłaszcza o środkach ochrony i zabezpieczeniach stosowanych w odniesieniu do Danych przez niego lub Administratora.
5. Podmiot przetwarzający zobowiązany jest niezwłocznie zastosować się do zaleceń Administratora dotyczących przetwarzania Danych, zwłaszcza dotyczących ich zabezpieczenia.
6. W miarę możliwości Podmiot przetwarzający udzieli pomocy Administratorowi w zakresie niezbędnym do odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
7. Podmiot przetwarzający zobowiązuje się do:
 - 1) udzielenia Administratorowi, na każde jego żądanie, wszelkich informacji niezbędnych do wykazania spełnienia obowiązków Podmiotu przetwarzającego wynikających z Aktów Prawnych, w terminie do 7 dni od dnia przyjęcia żądania;
 - 2) niezwłocznego, skutecznego poinformowania Administratora o:
 - a) każdym przypadku naruszenia ochrony Danych, tj. wszelkich sytuacjach stanowiących naruszenie Aktów Prawnych lub niniejszej umowy, zwłaszcza mogących skutkować odpowiedzialnością Administratora lub Podmiotu przetwarzającego na podstawie Aktów Prawnych (w tym o naruszeniu tajemnicy danych osobowych lub ich niewłaściwego wykorzystania), nie później jednak niż w ciągu 24 godzin od stwierdzenia danego zdarzenia. Powiadomienie wymaga formy pisemnej (w tym formy elektronicznej) pod rygorem nieważności,
 - b) każdym prawnie umocowanym żądaniu udostępnienia Danych właściwemu organowi państwa,
 - c) każdym żądaniu otrzymanym bezpośrednio od osoby, której dane przetwarza, w zakresie przetwarzania jej danych osobowych, powstrzymując się jednocześnie od odpowiedzi na żądanie, chyba, że zostanie do tego upoważniony przez Administratora,
 - d) jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający Danych,

- e) jakiegokolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych Danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych Danych, w szczególności prowadzonych przez inspektorów upoważnionych przez Urząd Ochrony Danych Osobowych.
8. Podmiot przetwarzający umożliwi pracownikom Administratora, odpowiednio przez niego umocowanym, dokonanie (w godzinach pracy Podmiotu przetwarzającego) sprawdzenia (w formie audytu/inspekcji) stanu ochrony i bezpieczeństwa Danych, pod kątem zgodności przetwarzania z Aktami Prawnymi oraz postanowieniami niniejszej umowy.
 9. Podmiot przetwarzający ma obowiązek współdziałać z pracownikami Administratora w czynnościach sprawdzających, o których mowa w ust. 8.
 10. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.
 11. Podmiot przetwarzający zobowiązuje się poinformować swoich pracowników o obowiązkach wynikających z Aktów Prawnych oraz o zobowiązaniach nałożonych niniejszą umową.

§ 5

Powierzenie wielopoziomowe

1. Podmiot przetwarzający może powierzyć Dane wynikające z niniejszej umowy do dalszego przetwarzania innemu podmiotowi przetwarzającemu, który musi spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w celu wykonania umowy, tylko po uzyskaniu uprzedniej pisemnej zgody Administratora.
2. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się z obowiązków spoczywających na innym podmiocie przetwarzającym, o którym mowa w ust. 1.
3. Przekazanie powierzonych Danych do państwa trzeciego lub organizacji międzynarodowej może nastąpić tylko na pisemne polecenie/zgodę Administratora. W przypadku posiadania takiego obowiązku prawnego przez Podmiot przetwarzający, przed podpisaniem umowy należy powiadomić o tym Administratora.

§ 6

Obowiązki i prawa Administratora

1. Administrator zobowiązuje się poinformować Podmiot przetwarzający o zamiarze przeprowadzenia audytu lub inspekcji w formie pisemnej (dozwolona wersja elektroniczna) na przynajmniej 7 dni roboczych przed planowanym terminem takiego sprawdzenia. Administrator dołoży starań, aby czynności wykonywane w ramach audytu lub inspekcji nie zakłócały działalności Podmiotu przetwarzającego.
2. Przedstawiciele Administratora są uprawnieni do wstępu do pomieszczeń, w których przetwarzane są Dane oraz do żądania od Podmiotu przetwarzającego udzielania informacji dotyczących przebiegu przetwarzania Danych.
3. Na zakończenie audytu lub inspekcji, o których mowa w ust. 1, przedstawiciel Administratora sporządza protokół w 2 egzemplarzach, który podpisują przedstawiciele obu stron. Podmiot przetwarzający może wnieść zastrzeżenia do protokołu w ciągu 5 dni roboczych od daty jego podpisania przez strony. Podmiot przetwarzający zobowiązuje się

dostosować do zaleceń Administratora, mających na celu usunięcie uchybień i poprawę bezpieczeństwa przetwarzania Danych w terminie wyznaczonym przez Administratora.

§ 7

Odpowiedzialność Podmiotu przetwarzającego

Podmiot przetwarzający ponosi pełną odpowiedzialność za wszelkie szkody, które powstaną wobec Administratora lub innych podmiotów i osób, w wyniku przetwarzania Danych niezgodnie z Aktami Prawa i umową. W szczególności obowiązek naprawienia szkody przez Podmiot przetwarzający dotyczy wszelkich szkód jakie poniesie Administrator, w szczególności pokrycia kosztów nałożonych kar, grzywien czy odszkodowań wynikających z orzeczeń właściwych organów.

§ 8

Okres obowiązywania umowy i warunki zakończenia współpracy

1. Niniejsza umowa zostaje zawarta na czas określony zgodny z okresem realizacji umowy, o której mowa w § 1 ust. 1.
2. Administrator ma prawo rozwiązać umowę bez zachowania terminu wypowiedzenia, gdy Podmiot przetwarzający:
 - 1) wykorzystał Dane w sposób niezgodny z umową,
 - 2) powierzył przetwarzanie Danych innemu podmiotowi przetwarzającemu bez zgody Administratora,
 - 3) jeśli w wyniku audytu lub inspekcji, o których mowa w § 4 zostanie stwierdzone, że Podmiot przetwarzający przetwarza Dane z naruszeniem Aktów Prawnych,
 - 4) nie zaprzestanie niewłaściwego przetwarzania Danych,
 - 5) w wyznaczonym terminie nie usunął uchybień, pomimo stwierdzonych podczas audytu lub inspekcji nieprawidłowości,
 - 6) zawiadomi o swojej niezdolności do dalszego wykonywania niniejszej umowy, a w szczególności niespełniania wymagań określonych w § 3 umowy.
3. Rozwiązanie umowy, o której mowa w § 1 ust. 1 skutkuje rozwiązaniem niniejszej umowy.
4. Po zakończeniu przetwarzania Danych na podstawie umowy, Podmiot przetwarzający zwróci Administratorowi na jego żądanie zgłoszone do 14 dni roboczych wszelkie materiały z Danymi i ich kopie, które pozostają w dyspozycji jego i innych podmiotów przetwarzających oraz podejmie odpowiednie działania, mające na celu wyeliminowanie możliwości dalszego przetwarzania Danych, w tym usunie Dane w sposób uniemożliwiający ich odtworzenie z wszelkich posiadanych przez siebie i innych podmiotów przetwarzających nośników informacji (w tym również z kopii zapasowych), chyba że Akty prawne nakazują przechowywanie danych osobowych.
5. Podmiot przetwarzający zobowiązuje się do niezwłocznego przekazania Administratorowi, na jego pisemne żądanie (dozwolona forma elektroniczna), protokołu z dokonania powyższych czynności.
6. W przypadku rozwiązania umowy, Podmiot przetwarzający zobowiązany jest do wykonania działań przewidzianych w przypadku zakończenia przetwarzania Danych.

§ 9

Postanowienia końcowe

1. W sprawach nieuregulowanych umową zastosowanie znajdują odpowiednie przepisy Aktów Prawnych, w szczególności Kodeksu cywilnego i Porozumienia.
2. Wszelkie zmiany umowy wymagają formy pisemnej pod rygorem nieważności i są dopuszczalne tylko w przypadku konieczności zapewnienia prawidłowej realizacji umowy i nadania jej zgodności z Aktami Prawnymi.
3. Po podjęciu wiedzy w przedmiocie nieważności jakichkolwiek postanowień umowy, Strony niezwłocznie sporządzą pisemny aneks do umowy, którym uchylą wadliwe postanowienia i w razie konieczności zastąpią je nowym brzmieniem.
4. Wszystkie spory, nieporozumienia czy roszczenia wynikłe lub powstałe w związku z wykonywaniem przedmiotu umowy, Strony będą starały się rozwiązać polubownie. Gdy polubowne rozstrzygnięcie nie zostanie osiągnięte, wszelkie spory wynikające z umowy będą rozstrzygane przez sąd powszechny właściwy miejscowo dla siedziby Administratora.
5. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

.....
ADMINISTRATOR

.....
PODMIOT PRZETWARZAJĄCY

ZAŚWIADCZENIE Nr/WAT/.....

**stwierdzające odbycie szkolenia
z zakresu ochrony danych osobowych**

Stwierdza się, że Pan(i):.....

(imię i nazwisko)

Jednostka organizacyjna:

odbył(a) szkolenie z zakresu ochrony danych osobowych przeprowadzone przez inspektora ochrony danych Wojskowej Akademii Technicznej na podstawie *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)* w:

**Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego
ul. Gen. Witolda Urbanowicza 2, 00-908 Warszawa 46**

(nazwa i adres siedziby jednostki organizacyjnej)

.....
Miejscowość i data

.....
*Imienna pieczęć i podpis
inspektora ochrony danych*

Ja, niżej podpisana/-y oświadczam, iż zostałam/-em przeszkolona/-y w zakresie ochrony danych osobowych, zapoznałam/-em się i rozumiem zasady dotyczące ochrony danych osobowych stosowane przez Wojskową Akademię Techniczną oraz zobowiązuję się do ich przestrzegania, a w szczególności do zachowania w tajemnicy danych osobowych oraz znanych mi sposobów zabezpieczenia danych osobowych stosowanych przez administratora danych, przez cały okres zatrudnienia/połączenia służby/świadczenia usług, jak również po ustaniu zatrudnienia /zakończenia pełnienia służby /świadczenia usług.

Oświadczam także, iż zostałam/-em poinformowana/-y o odpowiedzialności karnej i cywilnej za naruszenie przepisów z zakresu ochrony danych osobowych oraz zasad bezpieczeństwa stosowanych przez administratora danych.

.....
Imię i nazwisko,
data i podpis składającego oświadczenie

WZÓR INFORMACJI NA ŻĄDANIE

Warszawa, dnia

W związku z wystąpieniem Pana/Pani

.....

.....

.....

o dostęp do informacji w trybie art. 12 i w związku z art.15-22 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), uprzejmie informuję, że:

1. Administratorem danych jest:

Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego

ul. Gen. Witolda Urbanowicza 2, 00-908 Warszawa 46

Dane kontaktowe inspektora ochrony danych w WAT – email: iod@wat.edu.pl

2. Dane przetwarzane są w oparciu o:

- a) Art.

.....

.....

ustawy/rozporządzenia (np.: art. 6 pkt 1. a) RODO lub innej litery tego artykułu, bądź innego aktu prawnego),

celem:

.....

.....

.....

3. Odbiorcami Pana/Pani danych osobowych są (wybierz a lub/i b):

- a) pracownicy WAT realizujący statutowe zadania Uczelni,

- b)

4. Czas/okres przechowywania Pana/Pani danych (wybierz jedną lub kilka z opcji a, b, c lub d):

- a) zależy od czasu realizacji umowy,

- b) zależy od decyzji o archiwizacji dokumentacji należącej do WAT,

- c) dni/miesiący/lat,
d) inny (np. regulacja ustawowa):
.....
.....

5. Ma Pan/Pani prawo do żądania dostępu do swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych.
6. Jeżeli wcześniej osobiście Pan/Pani wyraził/a zgodę na przetwarzanie swoich danych osobowych istnieje prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.
7. Istnieje możliwość wniesienia skargi do organu nadzorczego.
8. Przekazane przez Pana/Panią dane były efektem (wybierz jedną z opcji a, b lub c):
- a) wymogu ustawowego,
b) warunkiem zawarcia umowy,
c) inny:.....
.....
9. Brak wyrażenia zgody na przekazanie danych osobowych, skutkowałby brakiem możliwości realizacji zadań WAT w relacji do Pana/Pani.

.....
Data i podpis specjalisty
ds. ochrony danych

UWAGA: Specjalista ds. ochrony danych bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania – udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem na podstawie art. 15–22 RODO. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania specjalista ds. ochrony danych informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.

Jeżeli specjalista ds. ochrony danych nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

Jeżeli specjalista ds. ochrony danych ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, o którym mowa w art. 15–22, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.

RAPORT Z NARUSZENIA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W WAT

- 1) Data: Godzina:
- 2) Osoba powiadamiająca o zaistniałym zdarzeniu:

(imię, nazwisko, stanowisko służbowe, nazwa użytkownika - jeśli występuje)
- 3) Zgodnie z art. 33 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), uprzejmie informuję, że istnieje uzasadnione podejrzenie naruszenia ochrony danych osobowych.
- 4) Lokalizacja zdarzenia:

(np. nr budynku, nr pokoju, nazwa/przeznaczenie pomieszczenia)
- 5) Charakter naruszenia danych osobowych:

- 6) Kategoria danych osobowych i przybliżona liczba osób, których dotyczy naruszenie ochrony danych osobowych:

- 7) Kategoria i przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie:

- 8) Potencjalne konsekwencje naruszenia danych osobowych:

- 9) Zastosowane lub proponowane środki w celu zaradzenia (zminimalizowania ewentualnych skutków) naruszenia ochrony danych osobowych:

- 10) Ewentualne uwagi dodatkowe (np. wyjaśnienie powodu opóźnienia przesłania informacji):

.....
Podpis osoby sporządzającej raport

INSTRUKCJA POSTĘPOWANIA W SYTUACJACH NARUSZENIA ZASAD OCHRONY DANYCH OSOBOWYCH

1. Celem niniejszej instrukcji jest określenie procedur postępowania w przypadku, gdy:
 - 1) stwierdzono naruszenie zasad zabezpieczenia w obszarze przetwarzania danych osobowych;
 - 2) stan urządzeń, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci komputerowej mogą wskazywać na naruszenie bezpieczeństwa danych osobowych.
2. Instrukcja określa zasady postępowania wszystkich osób mających dostęp do przetwarzania danych osobowych zarówno w systemach informatycznych oraz w wersji papierowej.
3. Naruszenie ochrony danych osobowych oznacza takie naruszenie zasad bezpieczeństwa, które prowadzi do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do przetwarzanych danych osobowych, a w szczególności:
 - 1) nieautoryzowany dostęp do danych;
 - 2) nieautoryzowane modyfikacje lub zniszczenie danych;
 - 3) udostępnienie danych nieautoryzowanym lub nieuprawnionym podmiotom;
 - 4) nielegalne ujawnienie danych;
 - 5) pozyskiwanie danych z nielegalnych źródeł.
4. W przypadku stwierdzenia lub podejrzenia naruszenia zabezpieczenia systemu lub zaistnienia zdarzeń, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każda osoba przetwarzająca dane osobowe w WAT jest zobowiązana przerwać przetwarzanie tych danych i niezwłocznie powiadomić o zaistniałym zdarzeniu bezpośredniego przełożonego, który poinformuje specjalistę ds. ochrony danych lub wyznaczonego przez niego LABI, a następnie powinien postępować stosownie do ich decyzji.
5. Specjalista ds. ochrony danych lub wyznaczony przez niego LABI analizuje zgłoszenie i w przypadku stwierdzenia naruszenia ma 12 godzin od momentu stwierdzenia naruszenia na jego zgłoszenie bezpośrednio do IOD.
6. AD zgłasza naruszenia organowi nadzorcemu w ciągu 72 godzin, chyba, że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
7. Jeżeli zgłoszenie naruszenia do organu nadzorczego nastąpi po upływie 72 godzin, AD zobowiązany jest wraz ze zgłoszeniem naruszenia przestać przyczynę opóźnienia zgłoszenia.

8. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, AD bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Zawiadomienie powinno być napisane jasnym i prostym językiem oraz opisywać charakter naruszenia według Formularza nr 1 Instrukcji postępowania w sytuacjach naruszenia zasad ochrony danych osobowych.
9. Jeżeli naruszenie dotyczy danych jednej lub kilku osób IOD udziela tym osobom wszelkich informacji dotyczącym naruszenia telefonicznie bądź mailowo.
10. Jeżeli naruszenie dotyczy danych wielu osób, AD ogłasza naruszenie do wiadomości publicznej poprzez komunikat w mediach/na stronie [www/w Biuletynie Informacji Publicznej](http://www.wbiuletynieinformacji publicznej). Ogłoszenie zawiera informację o kategorii osób, których dane zostały naruszone oraz o ich zakresie.
11. Zgłoszenie naruszenia procedur ochrony danych osobowych powinno zawierać:
 - 1) opis symptomów naruszenia procedur ochrony danych osobowych;
 - 2) określenie sytuacji i czasu zajścia zdarzenia;
 - 3) identyfikację rodzaju zaistniałego zdarzenia, w tym określenie skali zniszczeń, metody dostępu do danych osoby nieupoważnionej itp.;
 - 4) przedstawienie wszelkich istotnych informacji i dokumentów (wydruków, raportów, innych), mogących wskazywać na przyczynę naruszenia;
 - 5) określenie znanych danej osobie możliwości zabezpieczenia systemu oraz wszelkich działań podjętych po ujawnieniu zdarzenia w celu uniemożliwienia lub ograniczenia dostępu osób nieuprawnionych, minimalizacji szkód i zabezpieczenia śladów naruszenia ochrony danych.
12. Po stwierdzeniu naruszenia specjalista ds. ochrony danych lub wyznaczony przez niego LABI we współpracy z IOD podejmuje działania zmierzające do wyjaśnienia zgłoszonego zdarzenia. W zależności od rodzaju zgłoszonego zdarzenia może on dokonać w szczególności:
 - 1) wizji lokalnej w zakresie adekwatnym do rodzaju zgłoszonego zdarzenia;
 - 2) przeprowadzenia wywiadów z pracownikami w celu ustalenia okoliczności faktycznych;
 - 3) przeprowadzenia analizy poprawności funkcjonowania systemu informatycznego, jeżeli zgłoszone zdarzenie było związane z nieprawidłowym jego funkcjonowaniem;
 - 4) przeprowadzenia analizy zapisu zdarzeń w systemie informatycznym, z uwzględnieniem zapisu operacji realizowanych przez użytkowników;
 - 5) przeprowadzenia analizy danych przetwarzanych w systemie informatycznym, jeżeli zgłoszone zdarzenie mogło być spowodowane utratą dostępności lub integralności przetwarzanych danych;
 - 6) sporządzenia dokumentacji fotograficznej lub filmowej (w razie potrzeby);
 - 7) zabezpieczenia danych przetwarzanych w systemie informatycznym dotkniętym zdarzeniem, w szczególności danych konfiguracyjnych tego systemu;

- 8) zebrania innych materiałów pozwalających na wyjaśnienie przyczyn zaistnienia zdarzenia, jego charakteru i potencjalnych skutków.
13. Specjalista ds. ochrony danych lub wyznaczony przez niego LABI przy współpracy z ASI podejmują wszelkie działania mające na celu:
- 1) minimalizację negatywnych skutków zdarzenia;
 - 2) wyjaśnienie przyczyn i okoliczności zdarzenia;
 - 3) zabezpieczenie dowodów zdarzenia;
 - 4) zapewnienie możliwości dalszego bezpiecznego przetwarzania danych.
14. W celu realizacji zadań wynikających z niniejszej Instrukcji IOD, w porozumieniu ze specjalistą ds. ochrony danych oraz LABI, ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, a w szczególności:
- 1) żądania wyjaśnień od pracowników;
 - 2) korzystania z pomocy konsultantów;
 - 3) wnioskowania o wydanie zakazu wykonywania pracy w zakresie przetwarzania danych osobowych do czasu przywrócenia pożądanego bezpieczeństwa przetwarzania danych i zapewnienia przestrzegania procedur bezpieczeństwa;
 - 4) nakazania wprowadzenia dodatkowych środków bezpieczeństwa.
15. Polecenia IOD wydawane w czasie realizacji zadań wynikających z niniejszej instrukcji są priorytetowe i winny być wykonywane przed innymi, zapewniając ochronę danych osobowych.
16. Specjalista ds. ochrony danych lub wyznaczony przez niego LABI prowadzi rejestr naruszeń (incydentów) stanowiący Formularz nr 2 Instrukcji postępowania w sytuacjach naruszenia zasad ochrony danych osobowych.
17. Specjalista ds. ochrony danych lub wyznaczony przez niego LABI przesyła IOD rejestr zaistniałych incydentów.
18. IOD odpowiedzialny jest za przeprowadzanie przynajmniej raz w roku analizy zaistniałych incydentów w celu:
- 1) określenia skuteczności podejmowanych działań wyjaśniających i naprawczych;
 - 2) określenia wymaganych działań zwiększających bezpieczeństwo systemu informatycznego i minimalizujących ryzyko zaistnienia incydentów;
 - 3) określenia potrzeb w zakresie szkoleń z ochrony danych osobowych.
19. Odmowa udzielenia wyjaśnień lub współpracy z IOD w obszarze ochrony danych osobowych traktowana będzie jako naruszenie obowiązków pracowniczych.
20. IOD przy współdziałaniu z ASI oraz specjalistą ds. ochrony danych/LABI każdorazowo prowadzi szczegółową analizę i opracowuje w terminie 7 dni od daty zaistnienia zdarzenia raport, w którym przedstawia Rektorowi przyczyny i skutki zdarzenia oraz wnioski ograniczające możliwości wystąpienia podobnych zdarzeń w przyszłości wraz z propozycją konkretnych działań. Wzór raportu stanowi Formularz nr 3 Instrukcji postępowania w sytuacjach naruszenia zasad ochrony danych osobowych.

21. Nieprzestrzeganie zasad postępowania określonych w niniejszej Instrukcji stanowi naruszenie obowiązków pracowniczych i może być podstawą odpowiedzialności dyscyplinarnej określonej w *ustawie z dnia 26 czerwca 1974 r., Kodeks Pracy* (Dz. U. z 2018 r., poz. 108 z późn. zm).
22. Jeżeli skutkiem działania jest ujawnienie danych osobowych nieuprawnionej osobie lub podmiotowi, sprawca może zostać pociągnięty do odpowiedzialności karnej wynikającej z przepisów Kodeksu Karnego.

**Systemy i programy informatyczne
zastosowane do przetwarzania danych osobowych**

1. ZSI Egeria – w systemie przetwarzane są zbiory danych osobowych pracowników WAT pozostających w stosunku pracy, umów cywilno-prawnych (zlecenia i o dzieło), osób korzystających ze świadczeń socjalnych oraz żołnierzy zawodowych pełniących służbę w WAT.
2. USOS (Uniwersytecki System Obsługi Studiów) – w systemie przetwarza się zbiór danych osobowych pracowników, studentów cywilnych i wojskowych, doktorantów i słuchaczy studiów podyplomowych.
3. POL-on (System Informacji o Szkolnictwie Wyższym) – w systemie przetwarza się zbiór danych osobowych pracowników oraz studentów i doktorantów WAT.
4. SKD (System Kontroli Dostępu oparty na programie Andover Continuum i bazie Microsoft SQL Server) – w systemie przetwarza się zbiory danych osobowych osób z nadanymi uprawnieniami wejścia i przebywania w strefie obszaru chronionego WAT.
5. ALEPH (Automated Library Expandable Program) zintegrowany system, opracowany specjalnie dla potrzeb bibliotek, ośrodków informacji i archiwów. Systemu ALEPH500 w oparciu o bazę ORACLE oferuje pracę w trybie Klient-Serwer.
6. Płatnik (system oparty na bazie danych SQL) – w systemie przetwarza się zbiory danych osobowych osób będących płatnikami składek do ZUS.
7. Prosta K – w systemie przetwarza się zbiory danych osobowych żołnierzy zawodowych i służby okresowej w zakresie naliczania uposażeń.
8. LUZ – w systemie przetwarza się zbiory danych osobowych kandydatów na żołnierzy zawodowych w zakresie naliczania uposażeń.
9. BEZOF – system obecnie użytkowany tylko w celu pozyskania danych archiwalnych. System zawiera archiwalne dane osobowe osób, którym przyznano stypendia doktoranta oraz będące stroną zawartych umów cywilno-prawnych.
10. SORT – w systemie przetwarza się zbiory danych osobowych osób w celu ewidencji i rozliczania abonentów centrali telefonicznej WAT.
11. Mis-wynajem (system bazujący na aplikacji programu Lotus Notes) przeznaczony jest do ewidencji i obsługi wynajmu obiektów, pomieszczeń przez osoby lub firmy spoza WAT.
12. PKO - COLLECT (system bazujący na programie MS Excel) – przetwarzane są dane osobowe studentów w ramach opłat za zakwaterowanie w domach studenckich.
13. DN PLAZA – w systemie przetwarza się dane osobowe osób kwaterowanych w Domu Asystenta oraz przeznaczony jest do ewidencjonowania oraz prowadzenia rozliczeń finansowych z tego tytułu.

14. REKRUTACJA – w systemie przetwarza się dane osobowe kandydatów na studia I i II stopnia.
15. Program pakietu Microsoft Office tj.: Microsoft Word, Microsoft Excel i Microsoft Access.
16. System SMLZA – System Monitorowania Losów Zawodowych Absolwentów. W systemie przetwarzane są dane absolwentów Akademii do celów statystycznych.
17. MILNET-Z – niejawnny system informatyczny użytkowany w jednostkach organizacyjnych MON i nadzorowanych przez Ministra Obrony Narodowej. Wykorzystywany w Wojskowej Akademii Technicznej do przetwarzania danych osobowych żołnierzy zawodowych oraz kandydatów na żołnierzy zawodowych w zakresie obsługi kadrowej.

ZAKRES OBOWIĄZKÓW LOKALNEGO ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI

1. Lokalny administrator bezpieczeństwa informacji, zwany dalej: „LABI”, realizuje zadania w zakresie zapewnienia przestrzegania zasad przetwarzania i ochrony danych osobowych w ramach jednostek/komórek organizacyjnych będących we właściwości specjalisty ds. ochrony danych w zakresie przetwarzania danych osobowych.
2. LABI podlega bezpośrednio specjalście ds. ochrony danych.
3. Do podstawowych obowiązków LABI należy między innymi:
 - 1) prowadzić na bieżąco:
 - a) ewidencję wniosków o nadanie i cofnięcie uprawnień;
 - b) ewidencję osób upoważnionych do przetwarzania danych osobowych, wydanych/cofniętych upoważnień;
 - c) rejestry czynności przetwarzania danych;
 - d) rejestr udostępnionych danych;
 - e) rejestr naruszeń ochrony danych osobowych;
 - f) ewidencję wydanych upoważnień oraz złożonych oświadczeń o zapoznaniu z przepisami;
 - g) wykaz obszarów przetwarzania danych osobowych oraz opis przepływu danych osobowych pomiędzy poszczególnymi systemami.
 - 2) sprawować nadzór nad przestrzeganiem zasad przetwarzania i ochrony danych osobowych przetwarzanych w systemach informatycznych oraz w wersji papierowej;
 - 3) prowadzić okresowe (minimum raz w roku) i doraźne kontrole przestrzegania przez osoby przetwarzające dane osobowe, obowiązujących zasad ich przetwarzania, zabezpieczenia zbiorów oraz zgodności zakresu przetwarzania danych z udzielonym upoważnieniem oraz terminowego dokonywania zmiany haseł dostępu;
 - 4) podejmować odpowiednie działania w przypadku naruszenia zasad bezpieczeństwa, ujawnienia, zniszczenia, utraty danych osobowych lub podejrzenia naruszenia bezpieczeństwa danych osobowych, celem zminimalizowania skutków;
 - 5) wspierać IOD w nadzorowaniu zasad ochrony danych osobowych;
 - 6) zgłaszać IOD potrzeby szkoleniowe w zakresie ochrony danych osobowych;
 - 7) zgłaszać IOD dane do rejestrów czynności przetwarzania danych oraz informować o dotyczących zmianach w zakresie i sposobach przetwarzania;

- 8) sprawować nadzór nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe;
 - 9) współpraca z IOD oraz zgłaszanie mu problemów wynikających z realizacji zadań w jednostce organizacyjnej w zakresie ochrony danych osobowych;
 - 10) sprawować nadzór nad stosowanymi środkami zabezpieczającymi dane osobowe;
 - 11) uczestniczyć w organizacji i przeprowadzaniu szkolenia z przepisów i zasad bezpiecznego przetwarzania danych osobowych oraz prowadzić ewidencję uczestników szkolenia.
4. LABI ma prawo między innymi do:
- 1) dokonywania kontroli przestrzegania zasad przetwarzania i ochrony danych osobowych przetwarzanych w systemach lub programach informatycznych i poza systemami;
 - 2) wnioskowania do specjalisty ds. ochrony danych o dokonanie zmian w dokumentacji bezpieczeństwa: „*Polityce bezpieczeństwa danych osobowych w Wojskowej Akademii Technicznej*” i „*Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w WAT*”;
 - 3) nakazania usunięcia stwierdzonych uchybień w zakresie bezpieczeństwa przetwarzanych danych osobowych włącznie do wnioskowania do specjalisty ds. ochrony danych o cofnięcie upoważnienia do przetwarzania danych osobowych wobec osób naruszających zasady ich przetwarzania.

Wojskowa Akademia Techniczna
im. Jarosława Dąbrowskiego
ul. Gen. Witolda Urbanowicza 2
00-908 Warszawa 46

Szanowny/a Pan/Pani

**ZAWIADOMIENIE OSOBY, KTÓREJ DANE DOTYCZĄ
O NARUSZENIU OCHRONY DANYCH OSOBOWYCH**

W związku z art. 34 ust. 1 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), informuję o naruszeniu ochrony Pana/i danych osobowych przetwarzanych przez

Charakter naruszenia ochrony danych osobowych	
Możliwe konsekwencje naruszenia ochrony danych osobowych	
Środki zastosowane/proponowane w celu zaradzenia naruszeniu ochrony danych / zminimalizowania negatywnych skutków*	
Imię i nazwisko inspektora ochrony danych / punkt kontaktowy	

**W zależności od przypadku, który wystąpił.*

REJESTR NARUSZEŃ (INCYDENTÓW)

Lp.	Incydent lub zdarzenie	Źródło zgłoszenia	Data zgłoszenia	Przyczyna niezgodności	Działania korygujące i zapobiegawcze	Odpowiedzialny za realizację	Data zakończenia	Ocena skuteczności
1	2	3	4	5	6	7	8	9
2								
3								
4								
5								

.....
Sporządził: (data, podpis)

.....
Nazwisko, data i podpis specjalisty ds. ochrony danych

RAPORT O INCYDENCIE BEZPIECZEŃSTWA INFORMACJI

CZĘŚĆ A

ZGŁOSZENIE INCYDENTU

(wypełnia osoba zgłaszająca zdarzenie/incydent)

DANE OSOBY ZGŁASZAJĄCEJ INCYDENT:	
IMIĘ I NAZWISKO:	
ADRES e-mail:	
UŻYTKOWNIK SYSTEMU:	

OPIS ZDARZENIA

.....

.....

.....

.....

.....

KOMU ZGŁOSZONO INCYDENT:	
DATA I GODZINA ZGŁOSZENIA:	
PODPIS ZGŁASZAJĄCEGO:	

CZĘŚĆ B

DZIAŁANIA PO ZAISTNIENIU INCYDENTU

(wypełnia osoba rozpatrująca incydent)

IMIĘ I NAZWISKO:	
STANOWISKO SŁUŻBOWE:	
ADRES e-mail:	

KWALIFIKACJA JAKO INCYDENT

TAK
☐

NIE
☐

DATA I CZAS ZAJŚCIA INCYDENTU:	
-----------------------------------	--

DATA I CZAS WYKRYCIA INCYDENTU:	
DATA I CZAS ZGŁOSZENIA INCYDENTU	
MIEJSCE WYSTĄPIENIA INCYDENTU	

CHARAKTERYSTYKA INCYDENTU

KLASYFIKACJA

- ☐ nielegalne treści
- ☐ złośliwe oprogramowanie
- ☐ dostępność zasobów
- ☐ gromadzenie informacji
- ☐ próby włamań
- ☐ bezpieczeństwo informacji
- ☐ włamania
- ☐ inne (opisać)

WPŁYW INCYDENTU NA INFRASTRUKTURĘ SYSTEMU INFORMATYCZNEGO

WPŁYW INCYDENTU NA STAN ZBIORÓW

OPIS ROZWIĄZANIA PROBLEMU

ZAŁĄCZNIKI

IMIĘ I NAZWISKO:	
STANOWISKO SŁUŻBOWE:	
ADRES e-mail:	

WYNIKI POSTĘPOWANIA WYJAŚNIAJĄCEGO

(wypełnia osoba prowadząca postępowanie wyjaśniające)

- Czy incydent zakończony?

TAK

NIE

☐☐

- Czas trwania incydu:

- Czy powiadomiono Władze Akademii?

TAK

NIE

☐☐

- Wystąpienie incydu

celowe

przypadkowe

☐☐

USTALENIA

.....
.....

MOŻLIWOŚĆ NEGATYWNYCH PRZYSZŁYCH SKUTKÓW INCYDENTU

.....
.....

ZALECENIA W CELU PODNIESIENIA POZIOMU BEZPIECZEŃSTWA

.....
.....

ZAŁĄCZNIKI

.....

IMIĘ I NAZWISKO:	
STANOWISKO SŁUŻBOWE:	
DATA I PODPIS:	

NOTYFIKACJA NARUSZEŃ DO ORGANU NADZORCZEGO

1. Czy doszło do naruszenia bezpieczeństwa prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych?

TAK

NIE

☐☐

2. Czy naruszenie skutkuje ryzykiem naruszenia praw i wolności osób

fizycznych?

TAK

NIE

☐☐

Zgłoszenie naruszenia do organu nadzorczego*

*Należy wypełnić jeśli w pkt 1 i 2 wskazano TAK

OPIS CHARAKTERU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

.....

.....

OPIS MOŻLIWYCH KONSEKWENCJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

.....

.....

OPIS ZASTOSOWANIA LUB PROPONOWANYCH ŚRODKÓW W CELU ZMINIMALIZOWANIA NEGATYWNYCH SKUTKÓW/ZARADZENIA NARUSZENIA OCHRONY DANYCH OSOBOWYCH

.....

.....

DANE INSPEKTORA OCHRONY DANYCH

IMIĘ I NAZWISKO:	
DANE KONTAKTOWE:	

CZY ZGŁOSZONO NARUSZENIE DO ORGANU NADZORCZEGO W CIĄGU 72h?

TAK

NIE

☐☐

Wyjaśnienie opóźnienia do organu nadzorczego*

*Należy wypełnić jeśli wskazano NIE

.....

.....

Data zawiadomienia organu nadzorczego

Sposób zawiadomienia

Data i podpis inspektora ochrony danych

A. NOTYFIKACJA NARUSZEŃ OSOBIE, KTÓREJ DANE DOTYCZĄ

1. Czy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia lub wolności osoby, której dane dotyczą?

TAK

NIE

☐☐

Czy wystąpił wyjątek od notyfikacji naruszenia*

*Należy wypełnić, jeśli w pkt. 1 wskazano **TAK**

1. Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie

TAK NIE
☐ ☐

2. Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą

TAK NIE
☐ ☐

3. Obowiązek notyfikacji wymaga niewspółmiernie dużego wysiłku

TAK NIE
☐ ☐

Zgłoszenie naruszenia osobie, której dane dotyczą*

*Należy wypełnić jeśli w pkt 1 i 2 wskazano **TAK** a w pkt 3 **NIE**

OPIS CHARAKTERU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

.....
.....

OPIS MOŻLIWYCH KONSEKWENCJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

.....
.....

OPIS ZASTOSOWANIA LUB PROPONOWANYCH ŚRODKÓW W CELU ZMINIMALIZOWANIA NEGATYWNYCH SKUTKÓW/ZARADZENIA NARUSZENIA OCHRONY DANYCH OSOBOWYCH

.....
.....

DANE INSPEKTORA OCHRONY DANYCH

IMIĘ I NAZWISKO:	
DANE KONTAKTOWE:	

Data zawiadomienia osoby, której dane dotyczą

Sposób zawiadomienia

Data i podpis inspektora ochrony danych

WYDANIE KOMUNIKATU PUBLICZNEGO*

*Należy wypełnić jeśli w pkt 1 - 3 wskazano **TAK**

TREŚĆ KOMUNIKATU

.....
.....

DANE INSPEKTORA OCHRONY DANYCH

IMIĘ I NAZWISKO:	
DANE KONTAKTOWE:	

Data zawiadomienia osoby której dane dotyczą

Sposób zawiadomienia

Data i podpis inspektora ochrony danych

**INSTRUKCJA
ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM
SŁUŻĄCYM DO PRZETWARZANIA DANYCH
OSOBOWYCH W WAT**

Rozdział I

Postanowienia ogólne

§ 1

1. *Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w WAT* zwana dalej: „Instrukcją”, zawiera ogólne procedury zarządzania systemami informatycznymi oraz warunki i sposób postępowania przy wykorzystaniu systemów służących do przetwarzania danych osobowych w WAT zwanej dalej: „Wojskowa Akademia Techniczna”.
2. Celem Instrukcji jest podniesienie poziomu bezpieczeństwa systemów informatycznych, w których przetwarzane są dane osobowe z określeniem odpowiedzialności użytkowników za prawidłowe działanie tych systemów i bezpieczeństwo przetwarzania w nich danych.
3. Instrukcja została opracowana zgodnie z *Rozporządzeniem 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)* zwanym dalej: „RODO”.
4. Procedury, warunki i sposób postępowania, o których mowa w ust. 1, obowiązują wszystkich użytkowników systemów informatycznych, stosownie do przydzielonych uprawnień, zakresu obowiązków i odpowiedzialności.
5. W przypadkach uzasadnionych wymaganiami systemu informatycznego mogą być tworzone do tego systemu szczególne wymagania bezpieczeństwa i procedury bezpiecznej eksploatacji lub inne dokumenty.

§ 2

Podstawowe definicje

Przez użyte w niniejszej instrukcji określenia rozumie się:

- 1) **administrator** – zwany dalej: „administratorem danych” lub „AD” – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych (Wojskowa Akademia Techniczna reprezentowana przez Rektora);
- 2) **administrator systemu informatycznego** – zwany dalej: „ASI” – osoba odpowiedzialna za zapewnienie właściwego funkcjonowania systemu teleinformatycznego, przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu, przeciwdziałanie dostępowi osób trzecich do systemu oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w tym systemie;
- 3) **anonimizacja danych** – rozumie się przez to nieodwracalny proces polegający na tym, by nie istniała już możliwość wykorzystania danych do zidentyfikowania osoby fizycznej za pomocą „wszystkich sposobów, jakimi może się posłużyć”;
- 4) **bezpieczeństwo informacji** – rozumie się przez to zespół zasad, jakimi należy się kierować projektując oraz wykorzystując systemy i aplikacje służące do przetwarzania danych osobowych, aby dostęp do nich był zgodny z założeniami zasady privacy by design (nazywanej też „zasadą prywatności

w fazie projektowania”) oraz zasady privacy by default (nazywanej też „zasadą prywatności w ustawieniach domyślnych”);

- 5) **dane osobowe** – oznaczają 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 osoby fizycznej;
- 6) **elektroniczny nośnik** – elektroniczne urządzenie, na którym przechowuje się dane osobowe w celu ich ponownego odtworzenia w systemie informatycznym;
- 7) **hasło** – ciąg znaków literowych, cyfrowych lub innych specjalnych znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
- 8) **identyfikator użytkownika/login** – ciąg znaków literowych, cyfrowych lub innych specjalnych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych w systemie informatycznym;
- 9) **incydent** – rozumie się przez to naruszenie bezpieczeństwa danych osobowych;
- 10) **integralność danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- 11) **instrukcja/procedura** – dokument opisujący sposób postępowania i warunki realizacji jakiegoś działania lub grupy działań (procesów);
- 12) **inspektor ochrony danych** – zwany dalej: „IOD” – rozumie się przez to osobę wyznaczoną przez administratora w celu wsparcia AD w nadzorowaniu i przestrzeganiu zasad ochrony danych w Wojskowej Akademii Technicznej;
- 13) **kierownik jednostki organizacyjnej** – na potrzeby niniejszej Polityki zgodnie z Regulaminem organizacyjnym Wojskowej Akademii Technicznej oznacza: dziekana, dyrektora lub kierownika innej, niebędącej wydziałem jednostki organizacyjnej Wojskowej Akademii Technicznej, a także kierownika jednostki administracji centralnej – kierownika biura lub kierownika działu;
- 14) **naruszenie ochrony danych osobowych** – oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia lub zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych, przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
- 15) **obszar przetwarzania danych** – oznacza wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
- 16) **odbiorca** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią;

- 17) **opis przepływu danych** – oznacza opis przepływu danych między podmiotami przetwarzania przy wykorzystaniu systemów informatycznych;
- 18) **organ nadzorczy** – oznacza niezależny organ publiczny, ustanowiony przez państwo członkowskie UE;
- 19) **osoba nieuprawniona** – osoba, która nie powinna mieć dostępu do danych osobowych przetwarzanych w Wojskowej Akademii Technicznej;
- 20) **podmiot przetwarzający** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Wojskowej Akademii Technicznej;
- 21) **poufność danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom lub podmiotom;
- 22) **pracownik** – osoba pozostająca w stosunku pracy z Wojskową Akademią Techniczną na podstawie umowy o pracę, a także osoba wykonująca prace i czynności na podstawie umów innych niż umowa o pracę (w tym umów cywilnoprawnych oraz praktykanci, stażyści, wolontariusze) oraz żołnierze zawodowi pełniący zawodową służbę wojskową w WAT;
- 23) **profilowanie** – oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
- 24) **przetwarzanie** – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak 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 niszczenie;
- 25) **pseudonimizacja** – przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
- 26) **rozliczalność danych** – rozumie się przez to właściwość zapewniającą, że działania osoby lub podmiotu mogą być przypisane w sposób jednoznaczny tylko tej osobie lub podmiotowi;
- 27) **specjalista ds. ochrony danych** – zgodnie z zarządzeniem Rektora, prorektorzy, kanclerz, kierownicy podstawowych jednostek organizacyjnych;
- 28) **strona trzecia** – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;

- 29) **system informatyczny** – oznacza zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
- 30) **środki techniczne i organizacyjne** – oznacza środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych;
- 31) **usuwanie danych** – oznacza zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą – anonimizacja;
- 32) **uwierzytelnienie** – rozumie się przez to proces poprawnej identyfikacji użytkownika systemu informatycznego w stopniu umożliwiającym przyznanie odpowiednich uprawnień lub przywilejów w systemie informatycznym;
- 33) **użytkownik** – osoba posiadająca upoważnienie do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu;
- 34) **użytkownik systemu informatycznego** – osoba posiadająca upoważnienie do przetwarzania danych osobowych w systemie informatycznym w zakresie wskazanym w upoważnieniu, której nadano unikalny identyfikator i hasło;
- 35) **zabezpieczenie danych** – oznacza wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
- 36) **zagrożenie** – rozumie się przez to potencjalną możliwość wystąpienia incydentu;
- 37) **zasoby danych** – inaczej aktywa, wszystko co ma wartość dla WAT i służy przetwarzaniu informacji w tym dane osobowe przetwarzane w Wojskowej Akademii Technicznej;
- 38) **zbiór danych** – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
- 39) **zgoda osoby, której dane dotyczą** – oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, w którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

§ 3

Podstawowe zasady korzystania z systemów informatycznych

1. Przydzielony sprzęt oraz konta użytkownika w systemie informatycznym mają charakter służbowy i nie mogą być wykorzystywane do innych celów.
2. Użytkownik ponosi odpowiedzialność materialną za powierzony mu sprzęt informatyczny.
3. Użytkownik ponosi odpowiedzialność za zawartość i utrzymywanie w należytym porządku swoich katalogów na dyskach wbudowanych w stację roboczą oraz udostępnionych dyskach sieciowych.

4. Użytkownik może przechowywać wyłącznie pliki wykorzystywane w celach służbowych.
5. Poczta elektroniczna służy wyłącznie do celów służbowych. Użytkownik ma obowiązek regularnego odbierania, porządkowania i usuwania zbędnej poczty elektronicznej.
6. Użytkownik ma obowiązek przeskanowania programem antywirusowym wszystkich nośników danych pochodzących spoza Wojskowej Akademii Technicznej podłączonych do stacji roboczych/komputerów przenośnych we własnym zakresie.
7. Użytkownikowi zabrania się w szczególności:
 - 1) podejmowania czynności, które mogą zakłócić lub uniemożliwić prawidłowe funkcjonowanie sieci;
 - 2) korzystania z usług dostępu do Internetu w sposób, który narusza przepisy krajowe i międzynarodowe, np. w zakresie prywatności, praw autorskich, własności intelektualnej lub wszelkiego użycia, które narusza prawa osób trzecich i/lub może służyć działalności przestępczej;
 - 3) korzystania z zasobów nieetycznych, tj. stron www zawierających informacje, które są niezgodne z normami etycznymi, w szczególności promującymi przemoc, totalitaryzm, nienawiść, rasizm, rozpowszechniających pornografię, oferujących gry hazardowe, udostępniających nielegalne oprogramowanie oraz wszelkie materiały godzące w innych lub zakazane przez prawo;
 - 4) podejmowania prób korzystania z urządzeń, informacji i zasobów komputerowych, do których administrator systemu informatycznego nie przydzielił mu dostępu;
 - 5) dokonywania jakichkolwiek napraw i zmian w konfiguracji sprzętu.

Rozdział II

Stosowane metody i środki uwierzytelniania oraz procedury związane z zarządzaniem nimi i użytkowaniem

§ 4

1. Użytkownicy systemu informatycznego przetwarzającego dane osobowe wykorzystują w procesie uwierzytelniania identyfikator i hasło. Dla bezpieczeństwa przetwarzanych danych oraz ochrony użytkowników dopuszczalne jest stosowanie innych rozwiązań kryptograficznych, które uznawane są za silne.
2. Identyfikatory są przypisane użytkownikowi i nie podlegają zmianie.
3. Hasła użytkowników i inne dane uwierzytelniające podlegają szczególnej ochronie.
4. Hasła dostępu do systemu informatycznego muszą spełniać poniższe warunki:
 - 1) posiadać długość co najmniej 8 znaków,
 - 2) zawierać duże i małe litery,
 - 3) zawierać cyfry lub znaki specjalne.
5. Zmiana hasła użytkownika następuje nie rzadziej niż co 30 dni, chyba, że system wymusza zmianę hasła automatycznie. Hasło należy zmienić niezwłocznie

w przypadku podejrzenia, iż mogły się z nim zapoznać nieuprawnione osoby. Nowe hasło powinno różnić się od poprzednio używanych.

6. Użytkownik systemu informatycznego zobowiązany jest w szczególności do:
- 1) nieujawniania hasła innym osobom, w tym innym użytkownikom;
 - 2) zachowania hasła w tajemnicy, również po jego wygaśnięciu;
 - 3) niezapisywania hasła w miejscach widocznych;
 - 4) postępowania z hasłami w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym;
 - 5) przestrzegania zasad dotyczących jakości i częstotliwości zmian hasła;
 - 6) wprowadzenia hasła do systemu w sposób minimalizujący podejrzenie go przez innych użytkowników systemu.

§ 5

1. Osoby odpowiedzialne za zakup, zarządzanie oraz administrację systemów informatycznych w WAT, w których przetwarzane byłyby dane osobowe, zobowiązane są do stałego monitorowania i dokonywania zmian w systemach pod kątem ich zgodności z regulacjami prawnymi w zakresie ochrony danych osobowych. W przypadku konieczności zakupu przez WAT nowych systemów informatycznych, w których byłyby przetwarzane dane osobowe, należy kierować się zasadą uwzględniającą ochronę danych osobowych w fazie projektowania i zasadą domyślnej ochrony danych osobowych. Powyższa czynność wymaga wykazania zastosowania wymienionych reguł (**zasada rozliczalności**).
2. Przetwarzanie danych w systemach informatycznych opiera się na zasadach prywatności w fazie projektowania (privacy by design) i prywatności w ustawieniach domyślnych (privacy by default).
3. Zgodnie z zasadą privacy by design AD zobowiązany jest zapewnić już na etapie planowania nowych projektów systemów informatycznych wprowadzenie odpowiednich rozwiązań zapewniających ochronę danych użytkowników i ich przetwarzanie zgodnie z RODO.
4. Prywatność w fazie projektowania oznacza uwzględnianie ochrony danych już na etapie planowania nowych projektów systemów informatycznych, w szczególności z użyciem nowych technologii poprzez:
 - 1) wbudowaniu ochrony prywatności w każdy nowy system informatyczny, w procesy biznesowe m.in. przez jak najszybszą pseudonimizację danych;
 - 2) wbudowaniu ochrony prywatności w przepisy wewnętrzne WAT;
 - 3) uwzględnianiu ochrony danych osobowych na etapie przetargów publicznych;
 - 4) zasada privacy by default oznacza zagwarantowanie ustawień, które zapewniają ochronę danych, jako pierwotnych ustawień systemu informatycznego bądź oprogramowania. Ustawienia aplikacji bądź systemów przetwarzających dane osobowe, domyślnie powinny udostępniać minimalną ilość informacji o jego użytkowniku.
5. Prywatność w ustawieniach domyślnych polega między innymi na:

- 1) jak najdalej posuniętym zabezpieczeniu prywatności w ustawieniach początkowych każdego systemu;
 - 2) minimalizacja danych – przetwarzanie wyłącznie tych danych, które są niezbędne do osiągnięcia celu, dla którego zostały zebrane.
6. System informatyczny, w którym przetwarzane są dane osobowe – z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie – powinien zapewniać odnotowanie:
- 1) daty pierwszego wprowadzenia danych do systemu;
 - 2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzania w nim danych posiada wyłącznie jedna osoba;
 - 3) źródła danych, w przypadku zbierania danych, nie od osoby, której dotyczą;
 - 4) informacji o odbiorcach, w rozumieniu art. 4 pkt 9 *RODO*, którym dane osobowe zostały udostępnione, dacie i zakresie udostępnienia;
 - 5) sprzeciw osoby do przetwarzania jej danych osobowych.
7. Za realizację i przestrzeganie zasad bezpieczeństwa zawartych w Instrukcji, dla każdego systemu, w którym przetwarzane są dane osobowe odpowiada ASI.

Rozdział III

Procedury nadawania i cofania uprawnień do przetwarzania danych osobowych, rejestrowania tych uprawnień w systemie informatycznym oraz osoby odpowiedzialne za te czynności

§ 6

1. Celem procedury jest określenie zasad nadawania uprawnień do systemu informatycznego.
2. Osoba może być dopuszczona do przetwarzania danych osobowych w systemie informatycznym tylko wtedy, gdy posiada upoważnienie do przetwarzania danych osobowych.
3. Upoważnienia do przetwarzania danych osobowych nadawane są w związku z wykonywaniem przez upoważnioną osobę obowiązków lub zadań związanych z przetwarzaniem danych osobowych.
4. Podstawą do nadania uprawnień do przetwarzania danych osobowych w systemie informatycznym jest upoważnienie do przetwarzania danych osobowych.
5. Upoważnienie do przetwarzania danych osobowych wydaje AD lub specjalista ds. ochrony danych na wniosek kierownika jednostki organizacyjnej lub (jeśli ma to zastosowanie) specjalisty ds. ochrony danych. Sporządza się je w trzech egzemplarzach, jeden przeznaczony jest dla specjalisty ds. ochrony danych lub LABI jeśli został powołany, drugi dla osoby upoważnionej do przetwarzania danych osobowych, trzeci celem przekazania odpowiednio do Działu Personalnego lub Wydziału Kadr Wojskowych (do akt osobowych osoby upoważnionej). Kopię przedmiotowego upoważnienia specjalista ds. ochrony danych/LABI przekazuje ASI.

6. ASI zgodnie z otrzymanym upoważnieniem do przetwarzania danych osobowych, nadaje użytkownikowi systemu informatycznego uprawnienia w systemie, przydziela użytkownikowi identyfikator, potwierdza ten fakt poprzez złożenie na upoważnieniu czytelnego podpisu oraz wpisaniu daty i przekazuje go specjalście ds. ochrony danych/LABI.
7. Upoważnienia do przetwarzania danych osobowych rejestrowane są w ewidencji osób upoważnionych do przetwarzania danych osobowych prowadzoną przez specjalistę ds. ochrony danych/LABI.

§ 7

1. Każdy użytkownik posiadający upoważnienie do przetwarzania danych osobowych w systemie informatycznym otrzymuje od ASI, jednoznaczny i niepowtarzalny identyfikator do systemu oraz jednorazowe hasło tymczasowe. Po pierwszym poprawnym uwierzytelnieniu otrzymanym hasłem, wymuszana jest (przez system) zmiana hasła na docelowe hasło użytkownika, o złożoności zgodnej z niniejszą Instrukcją.
2. Identyfikator użytkownika i hasło tymczasowe do systemu informatycznego lub inne przyjęte metody uwierzytelniania (np. karta i kod PIN w systemie Security PKI) przekazywane są użytkownikowi w sposób uniemożliwiający zapoznanie się z nimi osób postronnych.
3. Podstawowym środkiem uwierzytelniania dostępu do systemu informatycznego służącego do przetwarzania danych osobowych jest identyfikator użytkownika i hasło dostępu do systemu. Obowiązują następujące zasady tworzenia hasła:
 - 1) nie może składać się z żadnych danych personalnych (imienia, nazwiska, adresu zamieszkania, nr PESEL itp. użytkownika, najbliższych osób itp.);
 - 2) musi składać się z co najmniej 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne;
 - 3) nie może składać się z identycznych znaków lub ciągu znaków z klawiatury;
 - 4) nie może być jednakowe z identyfikatorem użytkownika;
 - 5) musi być unikalne, tj. takie, które nie było poprzednio stosowane przez użytkownika.
4. Hasło w trakcie wpisywania, nie może być wyświetlane na ekranie. Użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności.
5. Zabronione jest zapisywanie lub przechowywanie haseł w miejscach niegwarantujących zachowania ich poufności.
6. Hasło musi być zmieniane nie rzadziej niż co 30 dni. Zmiana hasła w systemie informatycznym powinna być wymuszana przez system informatyczny przy logowaniu po upływie jego okresu ważności.
7. W przypadku podejrzenia utraty poufności hasła, użytkownik zobowiązany jest natychmiast poinformować o tym fakcie ASI i niezwłocznie zmienić hasło.
8. Identyfikator użytkownika nie może być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego służącego do przetwarzania danych osobowych nie może być przydzielany innej osobie.

9. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych osobowych, należy niezwłocznie zablokować w systemie informatycznym służącym do przetwarzania danych osobowych oraz unieważnić przypisane mu hasło.
10. Administrator systemu informatycznego prowadzi rejestr użytkowników systemu. W rejestrze odnotowuje się imię i nazwisko, identyfikator, zakres uprawnień użytkownika oraz datę nadania/modyfikacji/usunięcia uprawnień.
11. W przypadku konieczności odebrania lub zmiany zakresu uprawnień w systemie informatycznym kierownik jednostki organizacyjnej informuje ASI o konieczności wykonania powyższej czynności oraz podejmuje stosowne czynności dotyczące zmiany nadanego użytkownikowi upoważnienia.

§ 8

1. Cofnięcie uprawnień użytkownikowi w systemie informatycznym następuje w przypadku:
 - 1) zmiany przez osobę upoważnioną stanowiska lub jednostki organizacyjnej, w której jest zatrudniona lub pełni służbę;
 - 2) zmiany zakresu obowiązków w wyniku, której ustała konieczność przetwarzania danych osobowych;
 - 3) zawieszenia osoby w czynnościach służbowych;
 - 4) zwolnienia osoby ze służby, pracy lub zakończenia współpracy z WAT na podstawie umowy, porozumienia;
 - 5) cofnięcia upoważnienia lub upływu czasu, na który upoważnienie zostało udzielone.
2. W szczególnych wypadkach na wniosek kierownika jednostki organizacyjnej lub LABI oraz IOD uprawnienia użytkownika w systemie informatycznym mogą zostać zablokowane (zawieszone).
3. Wnioski o nadanie i cofnięcie uprawnień użytkownikowi w systemie informatycznym przechowuje i archiwizuje specjalista ds. ochrony danych lub LABI. Kopię wniosku może przechowywać i archiwizować także ASI, jeżeli takie rozwiązanie przyjęto dla danego systemu informatycznego.
4. Użytkownik zobowiązany jest do:
 - 1) posługiwania się własnym loginem i hasłem w celu uzyskania dostępu do systemów informatycznych;
 - 2) tworzenia haseł trudnych do odgadnięcia dla innych;
 - 3) używania konta służbowego wyłącznie w celach służbowych;
 - 4) nieprzerywania procesu skanowania przez program antywirusowy na komputerze;
 - 5) bieżącego wykonywania kopii zapasowych danych przetwarzanych na stanowisku komputerowym (pliki MS Office);
 - 6) zabezpieczenia przenośnego sprzętu komputerowego (smartfony, tablety, laptopy itp.) przed kradzieżą lub nieuprawnionym dostępem do danych.

Rozdział IV

Procedury rozpoczęcia, zawieszenia i zakończenia pracy systemu informatycznego służącego do przetwarzania danych osobowych

§ 9

1. Celem procedury jest określenie zasad dotyczących rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym w celu zapewnienia bezpieczeństwa danych osobowych w systemie informatycznym.
2. Przed rozpoczęciem przetwarzania danych osobowych użytkownik powinien sprawdzić, czy nie ma oznak fizycznego naruszenia zabezpieczeń. W przypadku wystąpienia jakichkolwiek nieprawidłowości, należy reagować zgodnie z instrukcją postępowania w sytuacjach naruszenia zasad ochrony danych osobowych.
3. Przed uruchomieniem stacji roboczej, użytkownik zobowiązany jest do upewnienia się, czy ekran monitora jest ustawiony w sposób uniemożliwiający osobom nieupoważnionym podglądanie jego zawartości.
4. Każde rozpoczęcie pracy w danym systemie wymaga logowania.
5. W przypadku problemów z rozpoczęciem pracy, spowodowanych odrzuceniem przez system wprowadzonego identyfikatora i hasła, należy skontaktować się z ASI.
6. W przypadku problemów podczas pracy z aplikacją przetwarzającą dane osobowe należy reagować zgodnie z instrukcją postępowania w sytuacjach naruszenia zasad ochrony danych osobowych.
7. Przystępując do pracy w systemie informatycznym służącym do przetwarzania danych osobowych, użytkownik zobowiązany jest w sposób dyskretny, aby nie było możliwości obserwacji klawiatury przez osoby postronne, wprowadzić swój identyfikator oraz hasło dostępu. Zabrania się wykonywania jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych z wykorzystaniem identyfikatora i hasła dostępu innego użytkownika.
8. W trakcie pracy użytkownik powinien mieć otwarte tylko te aplikacje, które są niezbędne do wykonywania obowiązków służbowych.
9. W trakcie pracy użytkownik powinien mieć na biurku tylko te materiały zawierające dane osobowe, które są niezbędne do wykonywania obowiązków służbowych.
10. W przypadku krótkotrwałego opuszczenia stanowiska pracy lub pomieszczenia, w szczególności, gdy w pomieszczeniu pracuje więcej niż jedna osoba, użytkownik systemu informatycznego jest zobowiązany uaktywnić wygaszacz ekranu zabezpieczony hasłem lub w inny sposób zabezpieczyć system przed dostępem innych osób.
11. Przebywanie osób nieuprawnionych w pomieszczeniach znajdujących się w obszarze przetwarzania danych osobowych, dopuszczalne jest tylko w obecności osoby upoważnionej do ich przetwarzania.
12. W przypadku trwającej dłużej niż 10 minut bezczynności użytkownika na stacji roboczej powinien być automatycznie włączany wygaszacz ekranu. Wznowienie pracy możliwe jest po ponownym uwierzytelnieniu.

13. W przypadku czasowego opuszczenia stanowiska pracy, użytkownik musi wylogować się z systemu informatycznego służącego do przetwarzania danych osobowych.
14. Zakończenie pracy w systemie służącym do przetwarzania danych osobowych powinno być poprzedzone sporządzeniem, w miarę potrzeb, kopii zapasowej danych oraz zabezpieczeniem ich przed nieuprawnionym dostępem osób nieuprawnionych.
15. Przed wylogowaniem należy sprawdzić, czy nie ma pozostawionych zadań do wydrukowania zarówno w pamięci komputera, jak i drukarki. W przypadku problemów powstałych podczas drukowania, wydrukować pustą (niezapisaną) stronę lub stronę testową. Jeżeli strona zostanie poprawnie wydrukowana, użytkownik może zakończyć pracę na stanowisku – w przeciwnym razie powiadamia ASI.
16. Przed opuszczeniem stanowiska pracy należy zabezpieczyć wykonane wydruki przed dostępem osób nieuprawnionych, bądź zniszczyć zbędne dokumenty w niszczarce. Należy skontrolować, czy w komputerze nie pozostały zewnętrzne nośniki danych.
17. Kończąc pracę w systemie informatycznym służącym do przetwarzania danych osobowych należy prawidłowo wylogować się z systemu informatycznego, wyłączyć komputer i zabezpieczyć stanowisko przed dostępem osób nieuprawnionych.
18. Zabrania się:
 - 1) kontynuowania uruchamiania systemu informatycznego, w sytuacji kiedy wystąpi jego nietypowe działanie, np. wyświetlanie niepokojących komunikatów itp.;
 - 2) eksploatacji systemu informatycznego działającego nieprawidłowo (anormalnie);
 - 3) kontynuowania pracy w przypadku, kiedy oprogramowanie antywirusowe wykryje obecność wirusa;
 - 4) zapisywania i pozostawiania w miejscach niezabezpieczonych przed ujawnieniem identyfikatora użytkownika i hasła (kodu PIN do karty PKI);
 - 5) ujawniania innym osobom identyfikatora użytkownika i hasła (udostępniania innym osobom karty PKI oraz kodu PIN);
 - 6) opuszczania pomieszczenia bez zabezpieczenia stanowiska pracy w sposób uniemożliwiający osobom postronnym dostęp do przetwarzanych danych osobowych;
 - 7) pozostawiania wydruków, wykorzystywanych dokumentów papierowych i informatycznych nośników danych bez nadzoru i zabezpieczenia przed dostępem i wglądem osób nieupoważnionych;
 - 8) wykonywania czynności wykraczających poza zakres nadanego upoważnienia do przetwarzania danych osobowych, w szczególności dokonywania nieuprawnionych prób dostępu do zasobów i dokonywania na nich wszelkich operacji;

- 9) wprowadzania bez zgody przełożonych osób nieuprawnionych do pomieszczeń, w których przetwarzane są dane osobowe;
 - 10) samowolnego uruchamiania i instalowania jakiegokolwiek oprogramowania;
 - 11) nieuprawnionego kopiowania jakichkolwiek danych znajdujących się w systemie informatycznym;
 - 12) samowolnej zmiany ustawień konfiguracyjnych sprzętu oraz przemieszczania urządzeń wchodzących w skład systemu informatycznego;
 - 13) używania na stanowiskach prywatnych nośników danych.
19. Opuszczając pomieszczenie, w którym przetwarzane są dane osobowe, pracownik zobowiązany jest do zamknięcia pomieszczenia na klucz.

Rozdział V

Procedura postępowania z wydrukami z systemów informatycznych

§ 10

1. Wydruki z systemu informatycznego zawierające dane osobowe mogą być sporządzane jedynie w związku z realizacją zadań i podlegają ochronie zgodnie z przepisami dotyczącymi ochrony danych osobowych oraz ich ewidencjonowaniu, przechowywaniu, przekazywaniu, archiwizacji i brakowaniu, zgodnie z obowiązującymi przepisami.
2. Wydruki z systemów informatycznych próbne i wadliwie wykonane, do czasu ich zniszczenia, należy chronić jak dokumenty właściwe.
3. Zniszczenia wydruków dokonuje się w sposób uniemożliwiający ich odtworzenie, przy użyciu przeznaczonych do tego celu urządzeń zgodnie z obowiązującymi przepisami.

Rozdział VI

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

§ 11

1. Celem procedury jest określenie zasad dotyczących wykonywania kopii zapasowych.
2. Za sporządzanie kopii zapasowych zbiorów danych przechowywanych na serwerach odpowiedzialny jest ASI, w którego właściwości pozostaje wykonywanie tych kopii.
3. Za kopie danych osobowych przetwarzanych na autonomicznych stanowiskach komputerowych odpowiadają użytkownicy.
4. Kopie zapasowe systemów, aplikacji baz danych i dokumentów użytkownika służą do zapewnienia możliwości odtworzenia w przypadku utraty aktualnie użytkowanych danych i/lub ponownej konfiguracji systemów i aplikacji.
5. Kopie zapasowe zbiorów danych powinny być wykonywane na odpowiednich nośnikach informacji i dokładnie opisanych. Kopie danych nie powinny być przechowywane w tych samych pomieszczeniach, w których znajdują się zbiory źródłowe.

6. Kopie zapasowe zbiorów danych należy wykonywać zgodnie ze specyfiką poszczególnych zbiorów danych. Częstotliwość i metodę wykonywania kopii zapasowych zbiorów danych określa ASI.
7. Dane przechowywane są na nośnikach przenośnych jedynie w przypadkach, gdy jest to konieczne, przez czas niezbędny do spełnienia celu, w jakim zostały one na nośniku zapisane. Po ustaniu czasu przechowywania zawartość nośnika danych podlega skasowaniu.
8. Dane osobowe w systemie informatycznym przechowywane są przez czas wymagany do spełnienia celu, dla którego są one przetwarzane. Po upływie tego celu dane podlegają skasowaniu lub anonimizacji.
9. Nośniki informatyczne zawierające dane osobowe lub kopie systemów informatycznych służących do przetwarzania danych osobowych są przechowywane w sposób uniemożliwiający ich utratę, uszkodzenie lub dostęp osób nieuprawnionych.
10. W celu zweryfikowania poprawności danych przechowywanych na kopiach zapasowych oraz możliwości przywrócenia za ich pomocą systemu do stanu sprzed awarii, ASI zobowiązani są do wykonywania okresowych testów odtworzenia kopii zapasowych. Testy powinny być wykonywane nie rzadziej niż raz na kwartał. Wyniki testów powinny zostać udokumentowane.
11. Dane usunięte z systemu informatycznego w związku z „prawem do bycia zapomnianym”, a znajdujące się na kopii zapasowej, w wyniku awarii systemu i ich przywrócenia z takiej kopii zapasowej, wymagają natychmiastowego usunięcia po wgraniu z bazy produkcyjnej.
12. ASI są zobowiązani do wprowadzenia obligatoryjnej ochrony antywirusowej, a także zabezpieczenia zaporą sieciową, która obejmuje wszystkie stacje robocze.
13. Oprogramowanie antywirusowe powinno być skonfigurowane w sposób wymuszający automatyczne usuwanie wirusów, zaś w przypadku, gdy ich usunięcie jest niemożliwe, obejmowanie ich kwarantanną, okresowe skanowanie wszystkich dysków lokalnych, a także sporządzanie raportów oraz powiadamianie osoby odpowiedzialnej o wykrytych wirusach, robakach czy innym szkodliwym oprogramowaniu.
14. Użytkownicy zobowiązani są do sprawdzania programem antywirusowym wszelkich elektronicznych zewnętrznych nośników informacji.

Rozdział VII

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

§ 12

1. Dane osobowe przechowywane są w postaci elektronicznej na:
 - 1) nośnikach elektronicznych wbudowanych w sprzęt informatyczny lub stanowiących element tego systemu;
 - 2) przenośnych nośnikach elektronicznych.
2. Dane przechowywane są na nośnikach przenośnych jedynie w przypadkach, gdy jest to konieczne, przez czas niezbędny do spełnienia celu, w jakim zostały one

na nośniku zapisane. Po ustaniu czasu przechowywania zawartość nośnika danych podlega skasowaniu.

3. Dane osobowe w systemie informatycznym przechowywane są przez czas wymagany do spełnienia celu, dla którego są one przetwarzane. Po upływie tego celu dane podlegają skasowaniu lub anonimizacji.
4. Wynoszenie nośników danych poza obszar przetwarzania danych osobowych, określony w *Polityce bezpieczeństwa danych osobowych w Wojskowej Akademii Technicznej* jest dozwolone tylko dla realizacji celów służbowych.
5. W przypadku zaistnienia okoliczności uzasadniającej konieczność wyniesienia nośników danych poza jednostkę organizacyjną, użytkownik zobowiązany jest do zachowania szczególnej ostrożności i zabezpieczenia nośnika, konieczne jest użycie środków ochrony kryptograficznej (szyfrowanie danych).
6. Za bezpieczeństwo komputerów przenośnych, urządzeń mobilnych, nośników danych odpowiadają ich użytkownicy. Zabrania się pozostawiania nośników danych bez nadzoru osoby upoważnionej.
7. Elektroniczne nośniki informacji zawierające dane osobowe oraz kopie zapasowe, a także wydruki i inne dokumenty zawierające dane osobowe przechowywane są w zamykanych na zamek szafach, w pomieszczeniach zlokalizowanych w obszarze przetwarzania danych osobowych, w sposób zabezpieczony przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem i zniszczeniem.
8. Nośniki informacji po upływie okresu ich użyteczności lub przechowywania, dane osobowe na nich zawarte powinny zostać skasowane tak, aby nie było możliwe ich odczytanie lub nośniki powinny być zniszczone. Nie należy przechowywać zbędnych nośników informacji oraz kopii zapasowych, a także wydruków i innych dokumentów zawierających dane osobowe.
9. W przypadku likwidacji nośników informatycznych zawierających dane osobowe lub kopie zapasowe systemów informatycznych służących do przetwarzania danych osobowych pozbawia się je zapisanych danych w sposób trwały, a w przypadku, gdy nie jest to możliwe, niszczy się w stopniu uniemożliwiającym ich odczytanie.
10. Zabrania się przekazywania na zewnątrz elektronicznych nośników informacji, na których uprzednio zapisane były dane osobowe. Można je powtórnie użytkować wyłącznie w strefie obszaru przetwarzania danych osobowych w WAT.

Rozdział VIII

Sposób zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych osobowych

§ 13

1. Systemy informatyczne służące do przetwarzania danych osobowych muszą być zabezpieczone przed szkodliwym oprogramowaniem.
2. Do ochrony przed działalnością szkodliwego oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych osobowych obowiązkowo stosowane jest oprogramowanie antywirusowe.

3. Wszystkie informatyczne nośniki danych z oprogramowaniem używanym w systemie (system operacyjny, programy użytkowe, oprogramowanie narzędziowe, sterowniki oraz pliki z danymi, w tym także wiadomość e-mail) podlegają procedurze kontroli na obecność wirusów. W przypadku wszelkich niejasności, podejrzeń należy kontaktować się z bezpośrednim przełożonym.
4. Na każdym stanowisku wyposażonym w dostęp do sieci Internet musi być zainstalowane oprogramowanie antywirusowe.
5. Niedopuszczalne jest stosowanie dostępu do sieci Internet bez aktywnej ochrony antywirusowej oraz zabezpieczenia przed dostępem szkodliwego oprogramowania. Zainstalowany program antywirusowy powinien być tak skonfigurowany, by dokonywane było automatycznie sprawdzenie komputera pod kątem obecności wirusów.
6. W przypadku stwierdzenia obecności wirusów, zabrania się samodzielnego ich usuwania przez użytkowników systemu. O incydencie należy niezwłocznie powiadomić bezpośredniego przełożonego.
7. ASI niezwłocznie podejmuje działania, mające na celu uniemożliwienie lub ograniczenie powstania szkód w wyniku działania wirusa, zabezpiecza zainfektowany nośnik danych w celu identyfikacji typu wirusa i ustalenie źródła infekcji. Postępuje zgodnie z instrukcją postępowania w sytuacjach naruszenia zasad ochrony danych osobowych.

Rozdział IX

Sposób odnotowania informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia

§ 14

1. Celem procedury jest określenie zasad związanych ze sposobem odnotowywania informacji w systemie informatycznym dotyczących udostępniania danych osobowych.
2. Dane osobowe udostępnia się osobom lub podmiotom uprawnionym do ich otrzymywania na mocy przepisów prawa. Zgodę na udostępnienie danych udziela specjalista ds. ochrony danych lub IOD.
3. W przypadku, gdy udostępniane są dane osobowe znajdujące się w zbiorach danych przetwarzanych w systemie informatycznym, system ten powinien umożliwić odnotowanie następujących informacji:
 - 1) numer wniosku i data udostępnienia;
 - 2) osoba lub podmiot, którym udostępnia się dane;
 - 3) podstawa prawna udostępnienia danych;
 - 4) zakres udostępnionych danych;
 - 5) imię i nazwisko osoby udostępniającej dane.
4. W przypadku przetwarzania danych w co najmniej dwóch systemach informatycznych, dopuszczalne jest odnotowywanie informacji, o których mowa w ust. 3, w jednym z nich.
5. W przypadku, gdy w systemie informatycznym służącym do przetwarzania danych osobowych nie jest możliwe odnotowywanie takich informacji, specjalista ds.

ochrony danych/LABI odnotowuje informacje wskazane w ust. 3 w prowadzonym rejestrze udostępnionych danych (Formularz nr 4 Polityki).

Rozdział X

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

§ 15

1. Przeglądy i konserwacje sprzętu komputerowego oraz nośników informacji służących do przetwarzania danych osobowych, przeprowadzane są w pomieszczeniach zlokalizowanych w obszarze przetwarzania danych osobowych, określonym w *Polityce bezpieczeństwa danych osobowych w Wojskowej Akademii Technicznej*.
2. Przegląd i konserwacja sprzętu informatycznego realizowane są przez uprawnionych pracowników Wojskowej Akademii Technicznej oraz przez podmioty zewnętrzne.
3. W przypadku przekazywania do naprawy sprzętu komputerowego z zainstalowanym systemem informatycznym służącym do przetwarzania danych osobowych lub nośnikiem informacji służącym do przetwarzania danych osobowych, powinien on zostać pozbawiony danych osobowych przez fizyczne wymontowanie dysku lub skasowanie danych, albo naprawa powinna zostać przeprowadzona w obecności osoby odpowiedzialnej za dany nośnik, ASI lub innej upoważnionej przez specjalistę ds. ochrony danych osoby. Należy spisać protokół przekazania sprzętu, który wskazuje osobę przekazującą oraz osobę odbierającą sprzęt.
4. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego wykonywane przez podmioty zewnętrzne, powinny odbywać się na zasadach określonych umową, z uwzględnieniem umowy powierzenia przetwarzania danych lub klauzul dotyczących zachowania danych w poufności przez wykonawcę usługi.
5. Za bezawaryjną pracę systemu informatycznego i aplikacji centralnych na poziomie jednostek organizacyjnych odpowiadają administratorzy tych systemów.
6. Przegląd i konserwacja urządzeń komputerowych oraz zmiany w systemach informatycznych wykonywane są według ustalonego planu, wynikającego z zaleceń producenta lub zgodnie z harmonogramem ustalonym przez ASI.
7. Nadzór nad przeprowadzaniem przeglądów technicznych, konserwacji i napraw sprzętu komputerowego, systemu informatycznego służącego do przetwarzania danych osobowych oraz nośników informacji służących do przetwarzania danych osobowych sprawuje ASI i specjalista ds. ochrony danych. ASI prowadzi dokumentację potwierdzającą wykonanie napraw, przeglądów i konserwacji.
8. Zabrania się:
 - 1) samowolnego przemieszczania pomiędzy pomieszczeniami, budynkami urządzeń elementów wchodzących w skład systemu informatycznego przeznaczonego do przetwarzania danych osobowych;
 - 2) samowolnej wymiany przez osoby nieuprawnione, w szczególności użytkowników systemu informatycznego, jakiegokolwiek elementu systemu informatycznego;
 - 3) samowolnego instalowania oprogramowania;

- 4) pozostawiania bez nadzoru informatycznych nośników danych, stanowiących element składowy systemu informatycznego, podczas przeglądów, konserwacji i naprawy systemu informatycznego.

Rozdział XI **Środki bezpieczeństwa**

§ 16

1. Wojskowa Akademia Techniczna stosuje środki bezpieczeństwa adekwatne do ryzyka związanego z przetwarzaniem danych osobowych.
2. Domyślnie wszystkie urządzenia, systemy informatyczne zapewniają najwyższą możliwą ochronę przetwarzania danych.
3. Środki bezpieczeństwa poddawane są przeglądom i aktualizacjom.
4. Zapisy dotyczące stosowania środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych określa Rozdział 14 *Polityki bezpieczeństwa danych osobowych w Wojskowej Akademii Technicznej*.
5. Wykaz zastosowanych środków bezpieczeństwa został opisany w rejestrze czynności przetwarzania danych osobowych.
6. Plan zapewnienia ciągłości działania i przywracania dostępności usług krytycznych dla funkcjonowania Wojskowej Akademii Technicznej został określony przez Dział Informatyki.

Rozdział XII **Pozostałe zasady ochrony systemu informatycznego służącego do przetwarzania danych osobowych**

§ 17

1. Należy instalować zalecane przez producentów oprogramowania poprawki i uaktualnienia systemu informatycznego służącego do przetwarzania danych osobowych celem wyeliminowania błędów w działaniu lub poprawienia wydajności działania.
2. Dostęp do BIOS-u komputera zabezpieczać należy hasłem ASI.
3. Należy wyłączyć możliwość ładowania się systemu stacji roboczej z zewnętrznych nośników (CD, DVD) lub urządzeń dołączonych poprzez USB.
4. W przypadku, gdy ze stacji roboczej korzysta więcej niż jeden użytkownik dostęp do systemu informatycznego powinien być zabezpieczony odrębnie dla każdego użytkownika, za pomocą przyjętych mechanizmów uwierzytelniania.
5. W systemie informatycznym podłączonym do sieci publicznej nie powinny być przechowywane zbiory danych lub przetwarzane dane osobowe, o których mowa w art. 9 ogólnego rozporządzenia o ochronie danych.
6. IOD, specjalista ds. ochrony danych, LABI i ASI ma prawo do kontroli stanu zabezpieczeń oraz przestrzegania zasad ochrony danych osobowych w dowolnym terminie.
7. W celu zabezpieczenia awaryjnego dostępu do systemu informatycznego przetwarzającego dane osobowe, kopia hasła ASI przechowywana jest w depozycie w miejscu wyznaczonym przez specjalistę ds. ochrony danych.

8. W uzasadnionych przypadkach specjalista ds. ochrony danych może wydać pisemne polecenie wykorzystania uprawnień ASI w trybie awaryjnym, przez upoważnioną osobę. Z konieczności skorzystania z uprawnień ASI w trybie awaryjnym sporządza się protokół dla IOD WAT.

Rozdział XIII

Procedura postępowania w sytuacji naruszenia bezpieczeństwa systemu informatycznego i przetwarzanych w nim danych osobowych

§ 18

1. Celem Procedury jest określenie zasad monitorowania i reagowania w sytuacji naruszenia ochrony danych osobowych;
2. Niniejsza procedura określa tryb i zasady postępowania osób przetwarzających dane osobowe, w przypadku gdy stwierdzono naruszenie ochrony danych osobowych;
3. Każda osoba przetwarzająca dane osobowe jest zobowiązana do reagowania zgodnie z instrukcją postępowania w sytuacjach naruszenia zasad ochrony danych osobowych w przypadku:
 - 1) stwierdzonym naruszeniu zabezpieczenia systemu informatycznego;
 - 2) wystąpieniu zagrożenia naruszenia bezpieczeństwa przetwarzanych danych osobowych w systemie informatycznym, w szczególności, gdy stan urządzenia, zawartość zbioru danych, zostały ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych.
4. Użytkownik systemu informatycznego w każdym przypadku naruszenia lub uzasadnionego podejrzenia naruszenia zabezpieczenia systemu informatycznego, w którym są przetwarzane dane osobowe, powinien:
 - 1) powstrzymać się od rozpoczęcia lub kontynuowania jakiejkolwiek czynności mogącej spowodować zatarcie śladów, bądź dowodów naruszenia;
 - 2) podjąć, stosownie do zaistniałej sytuacji, niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować naruszeniem danych osobowych.
5. Niezwłocznie po otrzymaniu informacji o naruszeniu lub o podejrzeniu naruszenia zabezpieczenia systemu informatycznego przetwarzającego dane osobowe, należy podjąć działania zmierzające do usunięcia zagrożenia bezpieczeństwa tych danych zgodnie z instrukcją postępowania w sytuacjach naruszenia zasad ochrony danych osobowych.

§ 19

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Zawiadomienie nie jest wymagane, w następujących przypadkach:
 - 1) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie,

uniemożliwiający odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

- 2) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w pkt 1;
 - 3) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.
2. Specjalista ds. ochrony danych/LABI, ASI oraz IOD dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

Rozdział XIV

Procedura dotycząca używania urządzeń przenośnych

§ 20

1. Celem procedury jest określenie zasad związanych z używaniem urządzeń przenośnych.
2. Procedury postępowania z informatycznymi nośnikami danych, w tym ewidencjonowanie, oznaczanie, przechowywanie, archiwizacja i brakowanie, powinny być zgodne z przepisami dotyczącymi obiegu informacji, dokumentów i archiwizacji w WAT.
3. Korzystanie ze służbowych komputerów przenośnych w miejscach publicznych możliwe jest jedynie w warunkach minimalizujących ryzyko zapoznania się z danymi przez osoby nieuprawnione.
4. Służbowe komputery przenośne należy sprawdzać pod kątem zainstalowanego oprogramowania antywirusowego, zainstalowanego dodatkowego oprogramowania oraz aktualizacji oprogramowania.
5. Niedozwolone jest wykorzystywanie służbowego komputera przenośnego do celów prywatnych oraz udostępniania go osobom nieuprawnionym.
6. Użytkownik systemu informatycznego używający urządzenie przenośne zawierające dane osobowe, zobowiązany jest zachować szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych.
7. W przypadku utraty urządzenia przenośnego użytkownik zobowiązany jest do reagowania zgodnie z instrukcją postępowania w sytuacjach naruszenia zasad ochrony danych osobowych.
8. Użytkownik systemu informatycznego używający urządzenie przenośne zawierające dane osobowe w szczególności powinien:
 - 1) stosować ochronę kryptograficzną;
 - 2) zabezpieczyć dostęp do urządzenia przenośnego przynajmniej przy pomocy identyfikatora i hasła lub innego równoważnego zabezpieczenia;
 - 3) nie zezwalać na używanie urządzenia przenośnego przez osoby nieupoważnione;

- 4) zachować szczególną ostrożność przy podłączaniu urządzenia przenośnego do sieci publicznych.
9. Za wszelkie działania wykonywane na urządzeniu przenośnym odpowiada jego użytkownik.
10. Zabrania się:
 - 1) nieuprawnionego wnoszenia poza obszar przetwarzania danych osobowych, nośników zawierających dane osobowe;
 - 2) używania prywatnych informatycznych nośników danych;
 - 3) wykorzystywania służbowych informatycznych nośników danych do celów innych niż te, do których są przeznaczone.
11. Nakazuje:
 - 1) przechowywanie informatycznych nośników danych w sposób uniemożliwiający dostęp do nich osób nieuprawnionych;
 - 2) usuwanie z informatycznych nośników zbędnych danych osobowych, które nie są wykorzystywane do bieżącej działalności służbowej i nie podlegają archiwizacji.
12. Dopuszcza się powierzenie niszczenia nośników danych podmiotom zewnętrznym, pod warunkiem:
 - 1) zawarcia umowy powierzenia przetwarzania danych;
 - 2) zagwarantowania poufności danych przez usługodawcę;
 - 3) umożliwienia prowadzenia nadzoru nad powierzonymi danymi;
 - 4) udokumentowania faktu zniszczenia nośników danych protokołem.

Rozdział XV

Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem działania jest uzyskanie nieuprawnionego dostępu do systemu

§ 21

1. W celu zabezpieczenia systemu informatycznego przed działaniem niebezpiecznego oprogramowania zabrania się:
 - 1) uruchamiania jakiegokolwiek oprogramowania, które nie zostało zatwierdzone do użytku w Wojskowej Akademii Technicznej;
 - 2) korzystania z nośników przenośnych bez uprzedniego sprawdzenia programem antywirusowym;
 - 3) otwierania poczty elektronicznej, której tytuł nie ma związku z pełnionymi obowiązkami służbowymi.
2. W przypadku zauważenia objawów mogących wskazywać na obecność niebezpiecznego oprogramowania użytkownik jest zobowiązany reagować zgodnie z instrukcją postępowania w sytuacjach naruszenia zasad ochrony danych osobowych. Do powyższych objawów można zaliczyć:
 - 1) istotne spowolnienie działania systemu informatycznego;
 - 2) nietypowe działanie aplikacji;

- 3) nietypowe komunikaty;
 - 4) utratę, modyfikację, zablokowanie danych.
3. Droga przedostania się szkodliwego oprogramowania może być sieć publiczna, wewnętrzna sieć teleinformatyczna lub elektroniczne nośniki danych.
 4. System informatyczny jest zabezpieczony przed działaniem oprogramowania złośliwego przez:
 - 1) oprogramowanie antywirusowe;
 - 2) zaporę sieciową;
 - 3) aktualizację oprogramowania systemowego;
 - 4) konfigurację oprogramowania minimalizującą ryzyko naruszenia bezpieczeństwa.
 5. Stacje robocze, komputery przenośne oraz serwery objęte są ochroną w czasie rzeczywistym za pomocą oprogramowania antywirusowego oraz zapory, zapewniających integralność zasobów przetwarzanych w systemie informatycznym.
 6. Oprogramowanie antywirusowe uruchamia się wraz ze startem systemu. Program antywirusowy zapewnia ciągłe monitorowanie otrzymywanych i wysyłanych, a także uruchamianych plików pod kątem występowania oprogramowania złośliwego.
 7. Oprogramowanie antywirusowe aktualizowane jest automatycznie.
 8. Stacje robocze i komputery przenośne przynajmniej raz w miesiącu skanowane są całościowo pod kątem występowania na nich oprogramowania złośliwego.
 9. Użytkownicy systemu mają obowiązek skanowania każdego zewnętrznego elektronicznego nośnika danych, który chcą wykorzystać chyba, że system antywirusowy robi to automatycznie.
 10. Zakazuje się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia programem antywirusowym.
 11. Zabronione jest pobieranie z Internetu plików niewiadomego pochodzenia.
 12. W przypadku stwierdzenia pojawienia się wirusa i braku możliwości usunięcia go przez program antywirusowy, użytkownik powinien poinformować o tym fakcie bezpośredniego przełożonego i niezwłocznie zaprzestać wykonywania jakichkolwiek czynności w systemie informatycznym.
 13. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, administrator systemu informatycznego podejmuje działania zmierzające do usunięcia tego zagrożenia.
 14. W szczególności działania te mogą obejmować:
 - 1) usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego;
 - 2) odtworzenie plików z kopii zapasowych, po uprzednim sprawdzeniu, czy dane zapisane na kopiach zapasowych nie są zainfekowane;

- 3) samodzielną ingerencję w zawartość pliku – w zależności od posiadanych kwalifikacji lub kontakt z odpowiednim serwisem.
15. Zastosowano mechanizmy monitorujące przeglądanie Internetu przez użytkowników, które uwzględniają:
 - 1) blokowanie stron internetowych określonego typu;
 - 2) analizę przesyłanych informacji pod kątem niebezpiecznego oprogramowania.
16. Bezpieczna konfiguracja systemów informatycznych odbywa się zgodnie z instrukcjami przygotowanymi przez Dział Informatyki.

Rozdział XVI

Postanowienia końcowe

§ 22

1. *Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w WAT* stanowi wewnętrzną regulację Wojskowej Akademii Technicznej. Obowiązuje wszystkich użytkowników.
2. Przestrzeganie postanowień niniejszej Instrukcji przez użytkowników systemów stanowi podstawę bezpiecznego posługiwania się systemami informatycznymi WAT.
3. Postanowienia niniejszej Instrukcji mogą być modyfikowane zarządzeniem Rektora WAT.
4. Propozycje zmian może składać pisemnie każdy pracownik WAT, korzystając z drogi służbowej lub bezpośrednio do IOD WAT.
5. IOD, specjalista ds. ochrony danych, ASI oraz LABI są zobowiązani do okresowego monitorowania przestrzegania przez pracowników zasad, przepisów i zarządzeń wewnętrznych dotyczących ochrony danych osobowych w WAT.
6. Naruszenie procedur ochrony danych przez pracowników zatrudnionych na podstawie umowy o pracę upoważnionych do przetwarzania danych osobowych może być potraktowane jako naruszenie obowiązków pracowniczych, włącznie z rozwiązaniem stosunku pracy (w tym bez wypowiedzenia) na podstawie przepisów ustawy z dnia 26 czerwca 1974 r., Kodeks Pracy (Dz. U. z 2018 r., poz. 108 z późn. zm).
7. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy *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)*, inne przepisy Unii Europejskiej, prawa krajowego oraz wewnętrzne akty prawne regulujących ochronę danych osobowych.
8. Wszystkie osoby przetwarzające dane osobowe w WAT zobowiązane są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w *„Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w WAT”*.

Sporządziła Maria Meszyńska – IOD WAT