Znak sprawy: RR11.0210.31.2024

Politechnika Śląska

Monitor Prawny Politechniki Śląskiej

poz. 91

ZARZĄDZENIE NR 27/2024
REKTORA POLITECHNIKI ŚLĄSKIEJ
z dnia 5 lutego 2024 r.

w sprawie Polityki ochrony danych osobowych na Politechnice Śląskiej

Na podstawie art. 23 ust. 1 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (j.t. Dz. U. z 2023 r. poz. 742, z późn. zm.), w związku 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) (Dz.U.UE.L.2016.119.1) oraz ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (j.t. Dz. U. z 2019 r. poz. 1781), zarządza się, co następuje:

§ 1

Wprowadza się Politykę ochrony danych osobowych na Politechnice Śląskiej stanowiącą załącznik do niniejszego zarządzenia.

§ 2

Traci moc zarządzenie nr 181/2023 Rektora Politechniki Śląskiej z dnia 4 października 2023 r. w sprawie Polityki ochrony danych na Politechnice Śląskiej (Monitor Prawny PŚ z 2023 r. poz. 1178).

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

Rektor PŚ: *A. Mężyk*

Polityka ochrony danych osobowych na Politechnice Śląskiej

Przepisy ogólne

§ 1

Polityka ochrony danych osobowych na Politechnice Śląskiej służy zapewnieniu ochrony danych osobowych przetwarzanych w Uczelni i zawiera:

1) zbiór regulacji i zasad dotyczących ochrony danych osobowych, których przestrzeganie zapewnia zgodność przetwarzania z wymaganiami ogólnego rozporządzenia o ochronie danych,
2) zadania i odpowiedzialności poszczególnych pracowników Politechniki Śląskiej w zakresie ochrony danych osobowych.

§ 2

Użyte w Polityce ochrony danych osobowych na Politechnice Śląskiej pojęcia oznaczają:

1) adekwatność danych — atrybut zapewniający, że dane są przetwarzane w zakresie minimalnym dla wypełnienia celu, dla którego zostały zebrane,
2) administrator danych osobowych (ADO) —Politechnikę Śląską reprezentowaną przez rektora,
3) administrator systemu informatycznego (ASI) – osobę wyznaczoną przez ADO, odpowiedzialną za funkcjonowanie systemów informatycznych wykorzystywanych do przetwarzania danych osobowych,
4) administrator danego systemu informatycznego – osobę odpowiedzialną za funkcjonowanie danego systemu informatycznego,
5) autoryzowane oprogramowanie – oprogramowanie dopuszczone do eksploatacji przez ADO,
6) BBI – Biuro Bezpieczeństwa Informacji,
7) dane osobowe —wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, 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,
8) dane osobowe szczególnych kategorii – dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące stanu zdrowia, seksualności lub orientacji seksualnej osoby fizycznej,
9) hasło – ciąg znaków znanych wyłącznie osobie uprawnionej, za pomocą którego użytkownik uzyskuje dostęp do systemu informatycznego,
10) incydent – zdarzenie mające lub mogące mieć wpływ na bezpieczeństwo przetwarzanych danych osobowych,
11) inspektor ochrony danych (IOD) — osobę powołaną przez ADO, wypełniającą zadania wynikające z art. 39 ogólnego rozporządzenia o ochronie danych,
12) integralność danych — atrybut zapewniający, że dane osobowe nie zostaną zmienione w sposób nieautoryzowany,
13) konto użytkownika – przestrzeń w systemie informatycznym, do której dostęp otrzymuje użytkownik; konto opatrzone jest hasłem, a nazwa konta stanowi login użytkownika; login jest unikatowy dla każdego użytkownika systemu i nie może być przypisany żadnemu innemu użytkownikowi,

14) lokalny administrator systemów informatycznych (LASI) – osobę odpowiedzialną za funkcjonowanie i prawidłową eksploatację całości systemów informatycznych w jednostce organizacyjnej lub pionie Politechniki Śląskiej,

15) lokalny pełnomocnik ochrony danych osobowych (LPODO) – osobę wyznaczoną przez kierownika jednostki/komórki organizacyjnej Politechniki Śląskiej, wspierającą go w wykonywaniu obowiązków wynikających z przepisów o ochronie danych osobowych,

16) naruszenie ochrony danych osobowych – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych,

17) Uczelnia – Politechnikę Śląską,

18) ustawa – ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych,

19) podmiot danych – osobę, której dane dotyczą,

20) Polityka ochrony danych osobowych na Politechnice Śląskiej – niniejszy dokument wraz z załącznikami,

21) poufność danych – atrybut zapewniający, że dane są przetwarzane wyłącznie przez osoby upoważnione przez ADO,

22) praca zdalna – pracę wykonywaną całkowicie lub częściowo w miejscu wskazanym przez pracownika i każdorazowo uzgodnionym z pracodawcą, w tym pod adresem zamieszkania pracownika, w szczególności z wykorzystaniem środków bezpośredniego porozumiewania się na odległość,

23) prezes UODO – Prezesa Urzędu Ochrony Danych Osobowych,

24) przetwarzanie danych osobowych — jakąkolwiek operację na danych osobowych, np.: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesyłanie, rozpowszechnianie lub innego rodzaju udostępnienie, dopasowanie lub łączenie, ograniczanie, usuwanie lub niszczenie,

25) RIG – Reed Into Green – oprogramowanie wprowadzone przez ADO do obsługi procesów zarządzania ochroną danych osobowych,

26) rozliczalność – umiejętność wykazania przestrzegania przepisów wynikających z ogólnego rozporządzenia o ochronie danych,

27) ogólne rozporządzenie o ochronie danych – rozporządzenie Parlamentu Europejskiego i Rady (UE) 216/679 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).

Rejestry

§ 3

1. Na Politechnice Śląskiej prowadzi się następujące rejestry:
   1) rejestr czynności przetwarzania – prowadzony na podstawie i zgodnie z zakresem art. 30 ust. 1 ogólnego rozporządzenia o ochronie danych,
   2) rejestr wszystkich kategorii czynności przetwarzania – prowadzony na podstawie i zgodnie z zakresem art. 30 ust. 2 ogólnego rozporządzenia o ochronie danych,
   3) rejestr umów powierzenia przetwarzania danych osobowych oraz współadministrowania,
   4) rejestr incydentów,
   5) rejestr upoważnień,
   6) rejestr realizacji praw osób, których dane są przetwarzane – prowadzony na podstawie art. 15, 16, 17, 18, 20, 21 i 22 ogólnego rozporządzenia o ochronie danych.
2. Do prowadzenia ww. rejestrów wykorzystywane jest dedykowane oprogramowanie dostarczane przez zewnętrznego dostawcę.
3. Rejestry, o których mowa w ust. 1 pkt 1 i 2, prowadzi inspektor ochrony danych na podstawie informacji przekazywanych przez LPODO oraz inicjatorów umów, kierowników projektów, koordynatorów projektów i inne osoby podejmujące nowy rodzaj przetwarzania danych osobowych w Uczelni.
4. Rejestry, o których mowa w ust. 1 pkt 3, 4 i 6, prowadzi BBI.

5. Rejestr upoważnień, o którym mowa w ust. 1 pkt 5, nadzoruje BBI, zaś wpisów w nim dokonują LPODO, z zastrzeżeniem § 6 ust. 9 Polityki ochrony danych osobowych na Politechnice Śląskiej.
6. Jeżeli wydawane są upoważnienia dla osób spoza Uczelni, wpisu do rejestru upoważnień dokonuje BBI po otrzymaniu skanu upoważnienia od inicjatora umowy, kierownika projektu lub koordynatora projektu.

Zasady przetwarzania danych osobowych

§ 4

Dane osobowe są przetwarzane z poszanowaniem następujących zasad:

1) zasady zgodności z prawem – wszystkie dane osobowe są gromadzone i przetwarzane przez Politechnikę Śląską na podstawie przesłanek wynikających z art. 6 ust. 1 ogólnego rozporządzenia o ochronie danych. W przypadku danych szczególnej kategorii musi istnieć przesłanka uchylająca ogólny zakaz przetwarzania tych danych, wynikająca z art. 9 ust. 2 ogólnego rozporządzenia o ochronie danych. Podstawy prawne przetwarzania danych osobowych zostały określone w rejestrze czynności przetwarzania. Osoba upoważniona przez ADO do przetwarzania danych osobowych nie może ich przetwarzać w innych celach oraz na podstawie innych przesłanek niż te wyszczególnione we wskazanym rejestrze,
2) zasady rzetelności i przejrzystości – dane osobowe są przetwarzane w sposób rzetelny i przejrzysty dla osoby, której dotyczą. Uczelnia wypełnia obowiązek informacyjny, który pozwala osobie, której dane dotyczą, poznać: dane kontaktowe ADO i IOD, cele, podstawy prawne ich przetwarzania oraz długość okresu przetwarzania danych, a także rodzaje przysługujących podmiotom praw w związku z przetwarzaniem danych osobowych oraz odbiorców danych. Informacje te muszą być przekazane osobom, których dane dotyczą, jasnym i prostym językiem, w przystępnej formie. W przypadku pozyskiwania danych osobowych od osoby, której one dotyczą, informacje te należy podać przed rozpoczęciem przetwarzania danych. W przypadku pozyskiwania danych z innych źródeł obowiązek informacyjny należy zrealizować najpóźniej w ciągu miesiąca od momentu pozyskania danych lub, jeśli dane te mają służyć do komunikacji z osobą, której dotyczą, obowiązek informacyjny należy zrealizować przy pierwszej takiej komunikacji, zachowując jednak termin nie późniejszy niż jeden miesiąc od pozyskania danych. Jeśli dane osobowe mają być ujawnione innemu odbiorcy, obowiązek informacyjny należy zrealizować przy pierwszym ujawnieniu, nie później jednak niż jeden miesiąc od momentu pozyskania danych. W przypadku pozyskiwania danych osobowych z innych źródeł niż od osoby, której one dotyczą, należy podać również źródło pozyskiwania danych,
3) zasady ograniczenia celu i minimalizacji danych – dane są gromadzone i przetwarzane wyłącznie w zakresie określonym przepisami prawa i niezbędnym do osiągnięcia celu określonego przez ADO. Wprowadza się bezwzględny zakaz przetwarzania danych osobowych bez aktualnej podstawy prawnej i poza rodzajami przetwarzań określonymi przez ADO. Zakres, rodzaje i cele przetwarzanych danych osobowych zostały przez ADO określone w rejestrze czynności przetwarzania oraz zostały określone w umowach powierzenia przetwarzania, gdzie Politechnika Śląska jest podmiotem przetwarzającym. Osoba upoważniona do przetwarzania danych osobowych nie może ich przetwarzać w szerszym zakresie oraz w innym celu niż te wyszczególnione we wskazanym rejestrze,
4) zasady ograniczenia przechowywania – dane osobowe podlegają przetwarzaniu wyłącznie do momentu osiągnięcia celu, w jakim zostały zebrane. Następnie są one archiwizowane i przechowywane zgodnie z okresem wyznaczonym w jednolitym rzeczowym wykazie akt obowiązującym na Politechnice Śląskiej. Po upływie wyznaczonego terminu dokumenty archiwalne podlegają ocenie i brakowaniu z zachowaniem zasady poufności danych. Dane osobowe można przechowywać przez okres dłuższy, o ile jest to przetwarzanie wyłącznie do celów archiwalnych, w interesie publicznym, do celów badań naukowych lub historycznych bądź do celów statystycznych na mocy art. 89 ust. 1 ogólnego rozporządzenia o ochronie danych, z zastrzeżeniem, że zostaną wdrożone odpowiednie środki techniczne i organizacyjne wymagane na mocy ogólnego rozporządzenia o ochronie danych w celu ochrony praw i wolności osób, których dane dotyczą,
5) zasady prawidłowości – prawidłowość i aktualność danych osobowych są na bieżąco weryfikowane. Pozyskiwanie danych osobowych może odbywać się wyłącznie od osób, których dane osobowe dotyczą, lub organów, które przekazują Uczelni dane osobowe na podstawie przepisów prawa. W wyjątkowych przypadkach pozyskiwanie danych osobowych może odbywać się od innych osób fizycznych niż osoby, których dane dotyczą. W przypadku powzięcia informacji o przetwarzaniu nieprawidłowych lub nieaktualnych danych osobowych, osoba przetwarzająca dane osobowe jest zobowiązana do ich korekty lub uaktualnienia. Jeżeli dane osobowe są przetwarzane przez więcej niż jedną osobę, osoba dokonująca korekty jest zobowiązana poinformować inne osoby, które również przetwarzają tego rodzaju dane

osobowe,
o dokonaniu ich korekty lub aktualizacji,

6) zasady poufności i integralności – administrator danych osobowych stosuje organizacyjne i techniczne środki ochrony danych w celu zachowania poufności, dostępności i integralność danych osobowych. Organizacyjne i techniczne środki ochrony danych osobowych przetwarzanych na nośnikach papierowych zostały wyszczególnione w § 7 Polityki ochrony danych osobowych na Politechnice Śląskiej. Organizacyjne i techniczne środki ochrony danych osobowych przetwarzanych w formie elektronicznej zostały zawarte w odrębnych dokumentach,
7) zasady rozliczalności – przetwarzanie danych osobowych może odbywać się wyłącznie według procedur opracowanych i wdrożonych w Uczelni, co podlega weryfikacji podczas audytów lub sprawdzeń przeprowadzanych przez inspektora ochrony danych oraz Biuro Audytu Wewnętrznego,
8) zasady przetwarzania danych osobowych do celów badań naukowych i prac rozwojowych:
   a) do przetwarzania danych osobowych przez Politechnikę Śląską do celów badań naukowych i prac rozwojowych wyłącza się stosowanie przepisów art. 15, 16, 18 i 21 ogólnego rozporządzenia o ochronie danych, jeżeli zachodzi prawdopodobieństwo, że prawa określone w tych przepisach uniemożliwią lub poważnie utrudnią realizację celów badań naukowych i prac rozwojowych i jeżeli wyłączenia te są konieczne do realizacji tych celów,
   b) w zakresie niezbędnym do prowadzenia badań naukowych i prac rozwojowych dopuszcza się przetwarzanie danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych bądź biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, a także danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby, jednak pod warunkiem, że publikowanie wyników tych badań i prac następuje w sposób uniemożliwiający identyfikację osoby fizycznej, której dane zostały przetworzone,
   c) dane osobowe, o których mowa w lit. a i b, poddaje się anonimizacji niezwłocznie po osiągnięciu celu badań naukowych lub prac rozwojowych. Do tego czasu dane, które można wykorzystać do identyfikacji danej osoby fizycznej, zapisuje się osobno. Można je łączyć z informacjami szczegółowymi dotyczącymi danej osoby fizycznej wyłącznie, jeżeli wymaga tego cel badań naukowych lub prac rozwojowych,
   d) do przetwarzania danych osobowych w celu przygotowania pracy dyplomowej lub rozprawy doktorskiej wymaganej do uzyskania odpowiednio dyplomu ukończenia studiów lub stopnia naukowego stosuje się zasady wynikające z lit. a-c.

Podstawy przetwarzania danych osobowych

§ 5

1. Dane osobowe na Politechnice Śląskiej są przetwarzane wyłącznie w przypadku, gdy spełniony jest co najmniej jeden z warunków:
   1) przetwarzanie danych osobowych jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy,
   2) przetwarzanie danych osobowych jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Uczelni. Przepis prawa będącego źródłem obowiązku, o którym mowa w zdaniu pierwszym, musi pochodzić z aktu prawnego o randze nie niższej niż ustawa lub z rozporządzenia, które zostało wydane na podstawie i w zakresie delegacji ustawowej. Obowiązek prawny może mieć swoje źródło w prawie krajowym lub unijnym,
   3) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej,
   4) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym,
   5) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Uczelnię,
   6) przetwarzanie jest oparte na zgodzie osoby, której dane dotyczą, jeśli nie zachodzi żadna z przesłanek wymienionych w pkt 1-5.
2. Podstawy przetwarzania danych osobowych, dla każdej czynności przetwarzania zidentyfikowanej na Politechnice Śląskiej, zawiera rejestr czynności przetwarzania.
3. Na Politechnice Śląskiej wprowadza się zakaz przetwarzania danych szczególnych kategorii.

4. Zakaz, o którym mowa w ust. 3, nie ma zastosowania, gdy zachodzą następujące okoliczności:
   1) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 3,
   2) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora danych osobowych lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą,
   3) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody,
   4) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń,
   5) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie oraz konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą,
   6) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego,
   7) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych bądź do celów statystycznych zgodnie z art. 89 ust. 1 ogólnego rozporządzenia o ochronie danych, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.
5. Zgoda jako podstawa przetwarzania może być pozyskiwana wyłącznie w sytuacji, w której ADO przewidział ją jako podstawę przetwarzania i zostało to ujęte w rejestrze, o którym mowa w § 3 ust. 1 pkt 1 Polityki ochrony danych osobowych na Politechnice Śląskiej.
6. Jednostka lub komórka organizacyjna realizująca zadania, których podstawą przetwarzania jest zgoda osoby, której dane dotyczą, jest zobowiązana do przechowywania zgód wraz z dokumentacją realizowanego zadania przez okres właściwy dla przechowywania tej dokumentacji, zgodnie z jednolitym rzeczowym wykazem akt obowiązującym na Politechnice Śląskiej.
7. Zapisy ust. 6 nie dotyczy projektów. W przypadku realizacji zadań projektu, których podstawą przetwarzania danych osobowych jest zgoda osoby, której dane dotyczą, zgody wraz z dokumentacją realizowanego zadania przechowuje kierownik projektu.

Procedura nadawania upoważnień do przetwarzania danych osobowych

§ 6

1. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie.
2. Upoważnienie wydaje się po przeszkoleniu z zakresu ochrony danych osobowych i po odebraniu oświadczenia o przyjęciu do wiadomości i stosowaniu zasad ochrony danych, w tym zasad opisanych w Polityce ochrony danych osobowych na Politechnice Śląskiej, a także po odebraniu oświadczenia o zachowaniu poufności. Szkolenie jest przeprowadzane przez LPODO przed wydaniem upoważnienia do przetwarzania danych osobowych.
3. Wzór upoważnienia stanowi załącznik nr 1 do Polityki ochrony danych osobowych na Politechnice Śląskiej.
4. Upoważnienie do przetwarzania danych osobowych jest wydawane przed przystąpieniem do wykonywania czynności służbowych bądź umownych. Zakres udzielonego upoważnienia jest nadawany stosownie do zakresu czynności powierzonych danemu pracownikowi lub zakresu działań związanych z realizacją umowy bądź w związku ze sprawowaną funkcją.
5. Pracownikom upoważnienie wydaje kierownik jednostki/komórki organizacyjnej, w której jest zatrudniony dany pracownik, a kierownikom jednostek/komórek organizacyjnych ich bezpośredni przełożony.
6. Upoważnienie do przetwarzania danych osobowych dla osób niebędących pracownikami wydaje osoba, która otrzymała pełnomocnictwo do zawarcia umowy, w ramach której wydawane są upoważnienia do przetwarzania danych osobowych.

7. Upoważnienia do przetwarzania danych osobowych dla studentów i doktorantów wydają odpowiednio dyrektor Centrum Obsługi Studiów i dyrektor Szkoły Doktorów.
8. Upoważnienie do przetwarzania danych osobowych w systemie POL-on wydaje rektor na wniosek uczelnianego administratora systemu POL-on. Wzór upoważnienia został określony w zarządzeniu w sprawie danych przetwarzanych w Zintegrowanym Systemie Informacji o Szkolnictwie Wyższym i Nauce POL-on.
9. Rejestr upoważnień, o których mowa w ust. 8, prowadzi uczelniany administrator systemu POL-on.
10. Upoważnienia do przetwarzania danych osobowych wydane pracownikom są przechowywane w aktach osobowych. Kierownik jednostki/komórki organizacyjnej jest zobowiązany do przekazania podpisanego przez pracownika upoważniania do Działu Zasobów Osobowych w terminie do 7 dni od dnia wydania upoważnienia.
11. Upoważnienia do przetwarzania danych osobowych dla osób niebędących pracownikami Politechniki Śląskiej są przechowywane wraz z dokumentacją związaną z realizacją umowy przez okres wskazany w jednolitym rzeczowym wykazie akt, właściwym dla tej dokumentacji.
12. Dla członków Samorządu Studenckiego upoważnienia są wydawane raz na cały okres kadencji tego gremium.
13. Upoważnienia do przetwarzania danych osobowych wydane studentom są przechowywane wraz z dokumentacją realizowanych zadań, w ramach których studenci przetwarzają dane osobowe.
14. Upoważnienia do przetwarzania danych osobowych wydaje się doktorantom na cały okres trwania studiów doktoranckich i przechowuje w dokumentacji osobowej doktoranta.
15. Wydawane upoważnienia podlegają ewidencji w rejestrze upoważnień nadzorowanym przez BBI.
16. LPODO jednostki lub pionu, w którym są wydawane upoważnienia, jest zobowiązany do wprowadzania ich do rejestru upoważnień, o którym mowa w ust. 15.
17. Każda osoba przetwarzająca dane szczególnych kategorii w procesach kadrowych musi posiadać pisemne upoważnienie do przetwarzania tych danych (art. 22^{1b} § 3 ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy).
18. Każda osoba przetwarzająca dane szczególnych kategorii w ramach administrowania zakładowym funduszem świadczeń socjalnych musi otrzymać pisemne upoważnienie ADO do przetwarzania tych danych w ramach tych czynności (art. 8 ust. 1b ustawy z dnia 4 marca 1994 r. o zakładowym funduszu świadczeń socjalnych).
19. Informację o upoważnieniach, o których mowa w ust. 17 i 18, zawiera się na ogólnym upoważnieniu do przetwarzania danych osobowych.
20. W przypadku zakończenia wykonywania zadań, w ramach których przetwarzane były dane osobowe, przez osobę legitymującą się upoważnieniem, o którym mowa w ust. 1, należy cofnąć wydane upoważnienie i powiadomić o tym fakcie BBI. Wzór cofnięcia upoważnienia stanowi załącznik nr 2 do Polityki ochrony danych osobowych na Politechnice Śląskiej.
21. Informację o cofnięciu upoważnienia wprowadza do rejestru upoważnień LPODO jednostki lub pionu, w którym zostało wydane cofnięcie upoważnienia.
22. Cofnięcie upoważnienia jest przechowywane w dokumentacji wraz z upoważnieniem.

Organizacyjne i techniczne środki ochrony danych osobowych przetwarzanych na nośnikach papierowych

§ 7

1. W pomieszczeniach, w których przetwarzane są dane osobowe, osoby postronne mogą znajdować się tylko w towarzystwie osób uprawnionych do przetwarzania danych.
2. Dokumenty zawierające dane osobowe są przechowywane w szafach/szufladach zamykanych na klucz.
3. Pomieszczenia, w których przetwarzane są dane osobowe, w czasie nieobecności osób zatrudnionych przy przetwarzaniu tych danych powinny być zabezpieczone poprzez zamknięcie drzwi na klucz.
4. Dostęp do kluczy do pomieszczeń, w których przetwarzane są dane osobowe, mają wyłącznie osoby uprawnione. Przed rozpoczęciem pracy klucze są pobierane od pracownika nadzorującego ich przechowywanie, zaś po zakończeniu pracy są zdawane w to samo miejsce.
5. Na Politechnice Śląskiej wprowadza się bezwzględny zakaz pozostawiania na biurku po skończonej pracy dokumentów zawierających dane osobowe. Dokumenty należy zabezpieczyć w sposób wskazany w ust. 2.
6. Dokumenty papierowe niepodlegające archiwizacji należy zniszczyć z użyciem niszczarki, w sposób uniemożliwiający ich ponowne odczytanie.

7. Drukarki i ksera znajdujące się w pomieszczeniach ogólnodostępnych są zabezpieczone hasłem przed dostępem osób nieuprawnionych.
8. Każdy pracownik korzystający z urządzeń powielających jest zobowiązany do sprawdzenia, czy w urządzeniu nie pozostał dokument zawierający dane osobowe.
9. W przypadku przewożenia lub przenoszenia dokumentów należy wprowadzić zabezpieczenia, które zapobiegną ich kradzieży, zagubieniu lub zniszczeniu.

Organizacyjne i techniczne środki ochrony danych osobowych przetwarzanych z użyciem systemów informatycznych

§ 8

Organizacyjne i techniczne środki ochrony danych osobowych przetwarzanych z użyciem systemów informatycznych regulują odrębne dokumenty.

Udostępnianie/powierzanie przetwarzania danych osobowych

§ 9

1. Udostępnienie danych osobowych instytucjom i osobom spoza Uczelni może odbywać się wyłącznie wtedy, gdy jest to wymagane lub dozwolone przepisami prawa lub za zgodą ADO.
2. Powierzenie przetwarzania danych osobowych może nastąpić wyłącznie podmiotowi przetwarzającemu gwarantującemu bezpieczeństwo przetwarzania danych osobowych.
3. Badanie gwarancji bezpieczeństwa powierzanych danych osobowych następuje z użyciem ankiety weryfikacyjnej podmiotu przetwarzającego. Wzór ankiety stanowi załącznik nr 3 do Polityki ochrony danych osobowych na Politechnice Śląskiej. Potencjalny podmiot przetwarzający jest zobowiązany do wypełnienia ankiety przed powierzeniem danych przez ADO. Scan ankiety jest dołączany do rejestru umów powierzenia przetwarzania prowadzonego przez BBI.
4. Umowa powierzenia przetwarzania danych osobowych musi zawierać wszystkie niezbędne regulacje wynikające z art. 28 ogólnego rozporządzenia o ochronie danych oraz deklarację stosowanych zabezpieczeń wynikających z art. 32 tego rozporządzenia. Umowa powinna zawierać w szczególności:
   1) określenie administratora danych osobowych i podmiotu przetwarzającego,
   2) rodzaj przetwarzania (rodzaj operacji wykonywanych na danych osobowych przez podmiot przetwarzający),
   3) czas trwania przetwarzania,
   4) charakter i cel przetwarzania,
   5) rodzaj danych osobowych oraz kategorie osób, których dane dotyczą,
   6) polecenie przetwarzania danych osobowych wydane przez administratora danych osobowych,
   7) warunki podpowierzenia danych (wymagana szczegółowa lub ogólna zgoda administratora danych osobowych),
   8) regulacje dotyczące ewentualnego przekazywania danych osobowych do krajów spoza Europejskiego Obszaru Gospodarczego,
   9) określenie i podział obowiązków pomiędzy administratorem danych osobowych a podmiotem przetwarzającym, dotyczących zabezpieczania danych osobowych (art. 32 ogólnego rozporządzenia o ochronie danych),
   10) regulacje dotyczące zgłaszania naruszeń danych osobowych,
   11) określenie sposobu postępowania z danymi osobowymi po zakończeniu trwania umowy,
   12) określenie warunków przeprowadzania czynności kontrolnych podmiotu przetwarzającego przez administratora danych osobowych, dotyczących przetwarzania danych osobowych mu powierzonych,
   13) informacje o obowiązku powiadomienia administratora danych osobowych przez podmiot przetwarzający w przypadku, gdy w jego ocenie administrator danych osobowych wydałby mu polecenie niezgodne z prawem.
5. W przypadku zaistnienia potrzeby powierzenia przetwarzania danych osobowych inicjator umowy przekazuje IOD projekt umowy wraz z listą kontrolną.
6. IOD zapoznaje się z umową i po wniesieniu ewentualnych uwag przekazuje ją do inicjatora umowy.

7. Umowa z uwagami naniesionymi przez inicjatora umowy również podlega kolejnej ocenie IOD.
8. W przypadku wniesienia przez kolejne jednostki widniejące na liście kontrolnej uwag i zaleceń co do treści umowy, które zmieniają sposób działania i mogą wpłynąć na charakter oraz zmianę warunków przetwarzania danych osobowych, inicjator umowy jest zobowiązany do poinformowania o tym IOD i przekazania aktualnej wersji do zaopiniowania przez IOD.
9. W przypadku gdy IOD nie wnosi żadnych uwag, przekazuje umowę wraz z listą kontrolną do akceptacji w kolejnych jednostkach.
10. Po podpisaniu zaakceptowanej umowy przez strony, inicjator umowy, w terminie do 7 dni, przesyła do BBI jej skan wraz z wypełnioną ankietą stanowiącą załącznik nr 4 do Polityki ochrony danych osobowych na Politechnice Śląskiej.

Prawo osób, których dane dotyczą

§ 10

1. Osoby, których dane dotyczą, mają następujące prawa:
   1) prawo do informacji,
   2) prawo dostępu do danych osobowych i otrzymania ich kopii,
   3) prawo do sprostowania i uzupełniania danych osobowych,
   4) prawo do usunięcia danych osobowych,
   5) prawo do ograniczenia przetwarzania danych osobowych,
   6) prawo do przenoszenia danych osobowych,
   7) prawo do sprzeciwu wobec przetwarzania danych osobowych,
   8) prawo do niepodlegania zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.
2. Prawo do informacji wskazane w ust. 1 pkt 1 należy realizować zawsze podczas pozyskiwania danych. Realizacja prawa do informacji następuje z inicjatywy administratora danych osobowych.
3. Prawa wskazane w ust. 1 pkt 2-8 realizuje się na wniosek osoby, której dotyczą przetwarzane dane.
4. Realizując prawo do informacji wynikające z art. 13 ogólnego rozporządzenia o ochronie danych podczas pozyskiwania danych od osób, których dane dotyczą, należy dołożyć starań, aby informacje przekazywane podmiotowi danych miały przejrzystą formę. Należy używać języka prostego i zrozumiałego dla odbiorcy komunikatu, w związku z czym:
   1) klauzula informacyjna powinna zawierać następujące obowiązkowe elementy:
      a) określenie administratora danych osobowych i jego dane kontaktowe,
      b) dane kontaktowe inspektora ochrony danych,
      c) cele przetwarzania danych osobowych oraz podstawę ich przetwarzania,
      d) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f ogólnego rozporządzenia o ochronie danych, należy przedstawić prawnie realizowany interes przez administratora danych osobowych lub stronę trzecią,
      e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeśli istnieją,
      f) informacje o zamiarze przekazania danych do państwa trzeciego i związanych z tym zabezpieczeniach danych,
      g) informacje na temat okresu przetwarzania danych osobowych, a jeśli nie jest to możliwe – kryteria ustalania tego okresu,
      h) informacje o prawie do żądania od administratora danych osobowych dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
      i) jeżeli przetwarzanie odbywa się na podstawie zgody (art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a ogólnego rozporządzenia o ochronie danych), należy przekazać informacje o prawie do cofnięcia zgody w dowolnym momencie, bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
      j) informacje o prawie do wniesienia skargi do organu nadzorczego,

k) informacje, czy przetwarzanie 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 profilowaniu, oraz informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą,

2) klauzulę informacyjną zamieszcza się:

a) na stronie internetowej administratora danych osobowych,

b) w biuletynie informacji publicznej,

c) przy wejściach na teren Uczelni (w przypadku stosowania monitoringu wizyjnego),

d) na drukach i formularzach, za pomocą których są zbierane po raz pierwszy dane osobowe,

e) jako informacje dodatkowe do umów i porozumień zawieranych przez Politechnikę Śląską,

f) w innych miejscach, zależne od kanału i sposobu komunikacji z osobą, której dane dotyczą,

3) informacje, o których mowa w art. 13 ogólnego rozporządzenia o ochronie danych, powinny być przekazywane przed pozyskiwaniem danych osobowych,

4) dopuszcza się również stosowanie warstwowego sposobu realizacji obowiązku informacyjnego. Osoba, której dane są przetwarzane, musi być poinformowana o administratorze danych osobowych, o celu przetwarzania jej danych osobowych oraz miejscu i sposobie uzyskania dodatkowych informacji wynikających z art. 13 ust. 1 i 2 ogólnego rozporządzenia o ochronie danych.

5. W przypadku prowadzenia postępowania o udzielenie zamówienia publicznego obowiązek informacyjny, o którym mowa w art. 13 ogólnego rozporządzenia o ochronie danych, można realizować poprzez zamieszczenie wymaganych informacji w ogłoszeniu o zamówieniu lub w dokumentach zamówienia.

6. Prowadząc postępowanie administracyjne, obowiązek informacyjny, o którym mowa w art. 13 ust. 1 i 2 ogólnego rozporządzenia o ochronie danych, jest realizowany przy pierwszej czynności skierowanej do strony, chyba że strona posiada te informacje, a ich zakres lub treść nie uległy zmianie.

7. Pozyskując dane osobowe ze źródeł innych niż osoba, której dane dotyczą, podmiotowi danych należy:

1) przedstawić wszystkie informacje określone w art. 14 ust. 1 i 2 ogólnego rozporządzenia o ochronie danych, tj.:

a) administratora danych osobowych oraz jego dane kontaktowe,

b) dane kontaktowe inspektora ochrony danych,

c) cele przetwarzania danych osobowych oraz podstawę prawną ich przetwarzania,

d) kategorie danych osobowych,

e) informacje o odbiorcach danych lub kategoriach odbiorców danych,

f) informacje o zamiarze przekazywania danych osobowych do państw trzecich wraz z wyszczególnieniem zabezpieczeń danych, które będą stosowane w związku ich przekazaniem,

g) informacje na temat okresu przetwarzania danych osobowych, a jeśli nie jest to możliwe – kryteria ustalania tego okresu,

h) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f ogólnego rozporządzenia o ochronie danych, należy przedstawić prawnie realizowany interes przez administratora danych osobowych lub stronę trzecią,

i) informacje o prawie do żądania od administratora danych osobowych dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,

j) jeżeli przetwarzanie odbywa się na podstawie zgody (art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a ogólnego rozporządzenia o ochronie danych), należy przekazać informacje o prawie do cofnięcia zgody w dowolnym momencie, bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,

k) informacje o prawie do wniesienia skargi do organu nadzorczego,

l) informacje o źródle pochodzenia danych oraz, gdy ma to zastosowanie, czy pochodzą one ze źródeł publicznie dostępnych,

m) informacje o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu, oraz informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

2) podać informacje, o których mowa w pkt 1:

a) najpóźniej w ciągu miesiąca od momentu otrzymania danych,

b) jeśli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – przy pierwszej takiej komunikacji, jednak nie później niż w ciągu miesiąca od pozyskania danych lub

c) jeśli planuje się ujawnić dane innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu, jednak nie później niż w ciągu miesiąca od pozyskania danych,

3) dopuszcza się również stosowanie warstwowego sposobu realizacji obowiązku informacyjnego. Osoba, której dane są przetwarzane, musi być poinformowana o administratorze danych osobowych, o celu przetwarzania jej danych osobowych oraz miejscu i sposobie uzyskania dodatkowych informacji wynikających z art. 14 ust. 1 i 2 ogólnego rozporządzenia o ochronie danych.

8. Realizacja prawa dostępu do danych wynikającego z art. 15 ogólnego rozporządzenia o ochronie danych wymaga:

1) potwierdzenia lub zaprzeczenia przetwarzania danych osobowych podmiotu danych,

2) jeżeli dane osobowe nie są przetwarzane – powiadomienia o tym fakcie wnioskodawcy (osoby, której dane dotyczą),

3) jeżeli dane osobowe są przetwarzane – przekazania osobie, której dane dotyczą, informacji określonych w art. 15 ust. 1 i 2 ogólnego rozporządzenia o ochronie danych, tj.:

a) celów przetwarzania,

b) kategorii danych osobowych,

c) informacji o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych,

d) informacji o planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe – kryteriach ustalania tego okresu,

e) informacji o prawie do żądania od administratora danych osobowych sprostowania, usunięcia lub ograniczenia przetwarzania danych oraz do wniesienia sprzeciwu wobec takiego przetwarzania,

f) informacji o prawie wniesienia skargi do organu nadzorczego,

g) jeżeli dane osobowe nie zostały zebrane od osoby, której dotyczą – wszelkich dostępnych informacji o ich źródle,

h) informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 ogólnego rozporządzenia o ochronie danych, oraz – przynajmniej w tych przypadkach – istotnych informacji o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą,

i) informacji o przekazywaniu danych do państwa trzeciego i związanych z tym zabezpieczeniach danych,

4) udzielenia dostępu do danych:

a) prawo dostępu do danych (dokumentów zawierających dane osobowe) jest udzielane wyłącznie w przypadku, gdy realizacja tego prawa nie będzie prowadzić do naruszenia praw i wolności innych osób,

b) każda forma udzielenia dostępu do danych musi zostać przeanalizowana pod kątem możliwego naruszenia praw i wolności innych osób fizycznych, których dane osobowe są przetwarzane w Uczelni,

5) w przypadku wniesienia żądania dostępu do danych przetwarzanych przez zamawiającego podczas prowadzenia procedury udzielania zamówienia publicznego zamawiający (administrator danych osobowych) może żądać od osoby występującej z takim wnioskiem wskazania dodatkowych informacji mających na celu sprecyzowanie nazwy lub daty zakończenia postępowania o udzielenie zamówienia,

6) wydania kopii danych przez administratora danych osobowych:

a) przez wydanie kopi danych osobowych rozumie się podanie informacji o zakresie przetwarzanych danych osobowych, chyba że wnioskujący doprecyzuje swoje żądanie,

b) wydanie kopii danych osobowych może nastąpić zarówno poprzez wydanie kopii nośnika danych osobowych, jak i poprzez podanie zakresu przetwarzanych danych osobowych,

c) wydanie kopii może odbywać się drogą elektroniczną, listownie lub do rąk własnych osobie wnioskującej,

d) jeżeli wniosek o realizację prawa dostępu do danych osobowych i wydanie ich kopii wpłynął drogą elektroniczną i zawierał zgodę (życzenie) na udzielenie informacji drogą elektroniczną, informacji udziela się w powszechnie stosowanej formie elektronicznej, po dokonaniu weryfikacji tożsamości wnioskującego.

9. Osobie, której dane dotyczą, przysługuje prawo do sprostowania danych wynikające z art. 16 ogólnego rozporządzenia o ochronie danych. Aktualne i poprawne dane osobowe są podstawą właściwej realizacji zadań administratora danych osobowych, a osoba, której dane dotyczą, ma prawo żądania od administratora danych osobowych wprowadzenia korekty jej danych oraz ich uzupełnienia, jeżeli uzna, że są one nieprawidłowe lub niekompletne. Realizacja wniosków odbywa się według poniższej procedury:
   1) wnioski podmiotów danych o sprostowanie i aktualizację danych osobowych powinny być realizowane niezwłocznie,
   2) o wprowadzeniu korekty danych osobowych należy poinformować wszystkich odbiorców danych, którym ujawniono dane osobowe,
   3) w przypadku gdy z wnioskiem wystąpi osoba, której dane dotyczą, należy ją poinformować o odbiorcach danych osobowych,
   4) w przypadku prowadzenia postępowania o udzielenie zamówienia publicznego skorzystanie przez osobę, której dane dotyczą, z prawa do sprostowania lub uzupełniania danych nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia ani zmianą postanowień umowy w sprawie zamówienia w zakresie niezgodnym z ustawą z dnia z dnia 11 września 2019 r. – Prawo zamówień publicznych,
   5) korzystanie z prawa do sprostowania lub uzupełniania danych osobowych nie może naruszać integralności protokołu oraz załączników z postępowania o udzielenie zamówienia,
   6) wnioski o sprostowywanie danych osobowych studentów należy przekazywać do Centrum Obsługi Studiów. Centrum Obsługi Studiów dokonuje korekty i informuje o tym wszelkie inne jednostki/komórki, które przetwarzają ten rodzaj danych osobowych,
   7) wnioski o sprostowanie danych osobowych pracowników należy przekazywać do Działu Zasobów Osobowych. Dział Zasobów Osobowych dokonuje korekty i informuje o tym wszelkie inne jednostki/komórki, które przetwarzają ten rodzaj danych osobowych,
   8) wnioski o sprostowanie danych osobowych doktorantów należy kierować do Szkoły Doktorów. Szkoła Doktorów dokonuje korekty i informuje o tym wszelkie inne jednostki/komórki, które przetwarzają ten rodzaj danych osobowych,
   9) wnioski o sprostowanie danych osób innych niż te wymienione w pkt 6-8 należy przekazywać do jednostek/komórek organizacyjnych, które przetwarzają ten rodzaj danych osobowych.
10. Osoba, której dane dotyczą, może wystąpić z wnioskiem o usunięcie jej danych osobowych zgodnie z art. 17 ogólnego rozporządzenia o ochronie danych, przy czym:
   1) usunięcie danych osobowych powinno nastąpić bez zbędnej zwłoki w przypadkach, gdy:
      a) dane nie są już niezbędne do celów, w których zostały zebrane,
      b) osoba, której dane dotyczą, cofnęła zgodę, na której oparte było przetwarzanie, i nie ma innej podstawy prawnej przetwarzania,
      c) dane były przetwarzane niezgodnie z prawem,
      d) osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ogólnego rozporządzenia o ochronie danych i nie zachodzi sytuacja, w której administrator danych osobowych jest w stanie wykazać prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec praw i wolności osób, których dane dotyczą lub podstaw do ustalenia, dochodzenia lub obrony roszczeń,
      e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator,
   2) jeżeli dane osobowe (np. wizerunek) zostały upublicznione, należy powiadomić administratorów, którym udostępniono dane, o żądaniu i zobowiązaniu do usunięcia tych danych, ich kopii i replikacji.
11. Osoba, której dane dotyczą, ma prawo żądać ograniczenia przetwarzania na podstawie art. 18 ogólnego rozporządzenia o ochronie danych:
   1) ograniczenie przetwarzania powinno nastąpić, gdy:

a) osoba, której dane dotyczą, kwestionuje prawidłowość danych – nie należy wówczas przetwarzać danych osobowych przez okres pozwalający sprawdzić ich prawidłowość,

b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystania,

c) administrator danych osobowych nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub ochrony roszczeń,

d) osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 ogólnego rozporządzenia o ochronie danych – nie należy wówczas przetwarzać danych osobowych do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora danych osobowych są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą,

2) ograniczenie przetwarzania polega na tym, że dane osobowe są wyłącznie przechowywane i nie są udostępniane ani w żaden inny sposób przetwarzane,

3) o uchyleniu ograniczenia przetwarzania danych osobowych administrator danych osobowych informuje osobę, której dane dotyczą,

4) jeżeli w toku prowadzenia postępowania o udzielenie zamówienia publicznego zostanie wniesione żądanie o ograniczenie przetwarzania danych osobowych na podstawie art. 18 ust. 1 ogólnego rozporządzenia o ochronie danych, nie ogranicza się przetwarzania danych osobowych do czasu zakończenia postępowania,

5) po zakończeniu postępowania o udzielenie zamówienia protokół z postępowania jest jawny i udostępniany na wniosek. Ograniczenie przetwarzania w protokole lub załącznikach do tego protokołu powoduje, że od dnia zakończenia postępowania zamawiający nie udostępnia tych danych, chyba że zachodzą przesłanki wynikające z art. 18 ust. 2 ogólnego rozporządzenia o ochronie danych, tj.:

a) przetwarzanie polega na przechowywaniu,

b) udostępnianie będzie miało miejsce wyłącznie za zgodą osoby, której dane dotyczą,

c) udostępnianie będzie miało na celu ustalenie lub obronę roszczeń,

d) udostępnienie nastąpi z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego,

6) nie udostępnia się danych szczególnych kategorii zawartych w protokole i zebranych w toku postępowania o udzielenie zamówienia.

12. Osobie fizycznej, która jest stroną umowy, oraz osobie, której dane są przetwarzane na podstawie zgody, przysługuje prawo do przenoszenia danych wynikające z art. 20 ogólnego rozporządzenia o ochronie danych. Prawo to jest realizowane w następujący sposób:

1) na żądanie osoby, należy przekazać jej dane do wskazanego administratora danych osobowych, używając jednego z następujących formatów: txt, csv, xml,

2) dopuszcza się także stosowanie innych formatów przekazywania danych osobowych, pod warunkiem jednak, że zastosowane formaty spełniają warunki interoperacyjności,

3) w przypadku fotografii stosuje się format jpg lub bmp,

4) jeżeli realizacja żądania osoby, której dane dotyczą, nie jest możliwa ze względów technicznych, stanowi to podstawę odmowy przeniesienia danych – należy wówczas przekazać osobie, której dane dotyczą, informację o odmowie wraz z jej uzasadnieniem.

13. Osoba, której dane dotyczą, ma prawo do sprzeciwu wynikające z art. 21 ogólnego rozporządzenia o ochronie danych:

1) osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw związany z jej szczególną sytuacją wobec przetwarzania jej danych osobowych, oparty na przesłance wynikającej z art. 6 ust. 1 lit e lub f ogólnego rozporządzenia o ochronie danych,

2) żądanie ograniczenia przetwarzania danych osobowych wymaga uzasadnienia ze strony osoby, której dane dotyczą,

3) w przypadku uwzględnienia sprzeciwu nie należy już przetwarzać danych osobowych objętych sprzeciwem,

4) dopuszcza się odmowę uwzględnienia sprzeciwu, jeżeli wykaże się istnienie ważnych, prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osób, których dane dotyczą, lub podstaw do ustalenia, dochodzenia i obrony roszczeń.

14. Osoba, której dane dotyczą, ma prawo do niepodlegania decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, wynikające z art. 22 ogólnego rozporządzenia o ochronie danych. Jeżeli

podejmowane są decyzje mające skutki prawne dla osoby, której dane dotyczą, w sposób zautomatyzowany, należy poinformować osobę, której dane dotyczą, spełniając obowiązek informacyjny, o prawie do wniesienia do rektora Politechniki Śląskiej odwołania od decyzji podjętej w sposób zautomatyzowany. Rektor rozpatruje wówczas argumenty osoby wnoszącej odwołanie i zmienia albo podtrzymuje podjętą wcześniej decyzję.

15. Realizacja praw osoby, której dane dotyczą, wynikających z rozdziału III ogólnego rozporządzenia o ochronie danych powinna następować bez zbędnej zwłoki, nie później jednak niż w ciągu miesiąca od otrzymania żądania. Okres ten można przedłużyć o kolejne dwa miesiące ze względu na obiektywne trudności w realizacji żądania. W przypadku wydłużenia terminu załatwiania sprawy należy powiadomić o tym stronę wnoszącą żądanie oraz przedstawić uzasadnienie wydłużenia terminu.
16. W toku prowadzenia postępowania o udzielenie zamówienia informacja o ograniczeniach stosowania przepisów ogólnego rozporządzenia o ochronie danych musi zostać zawarta w ogłoszeniu o zamówieniu, w dokumentach zamówienia lub być zakomunikowana w innej formie.
17. Informacje o realizacji praw, o których mowa w § 11 ust. 1 pkt 2-8 Polityki ochrony danych osobowych na Politechnice Śląskiej, jednostka/komórka organizacyjna powinna przesłać do BBI w terminie 7 dni od dnia realizacji żądania osoby wnioskującej.

Szkolenia z zakresu ochrony danych osobowych

§ 11

1. Pracownicy przetwarzający dane osobowe są zobowiązani do uzyskania odpowiedniej wiedzy z zakresu bezpieczeństwa przetwarzania danych osobowych, koniecznej do wykonywania zadań służbowych.
2. Obowiązkowi odbycia szkoleń podlegają wszyscy pracownicy również praktykanci i stażyści odbywający praktykę / staż w Uczelni, podczas której będą przetwarzać dane osobowe.
3. Szkolenia mogą mieć formę e-learningową lub z bezpośrednim udziałem uczestników.
4. W przypadku nowo zatrudnianych pracowników szkolenie odbywa się przed dopuszczeniem do wykonywania czynności służbowych. Szkolenie odbywa się z użyciem Platformy Zdalnej Edukacji. LPODO wyznaczony dla jednostki zatrudniającej pracownika, przekazuje do teczki akt osobowych pracownika potwierdzenie odbycia szkolenia.
5. Szkolenia stażystów, praktykantów i wolontariuszy odbywają się na takich samych zasadach jak szkolenia pracowników.
6. Szkolenia dla członków Samorządu Studenckiego i Samorządu Doktorantów przeprowadza się przed rozpoczęciem kadencji.
7. LPODO są odpowiedzialni za przeprowadzanie i nadzór nad terminowym odbyciem szkolenia z zakresu ochrony danych osobowych, odpowiednio w poszczególnych jednostkach/komórkach organizacyjnych Uczelni.

Postępowanie w sytuacji wystąpienia incydentu lub naruszenia danych osobowych

§ 12

1. Każdy pracownik jest zobowiązany do zgłaszania wszelkich sytuacji niebezpiecznych, mogących skutkować naruszeniem bezpieczeństwa danych. Przyjmuje się, że incydent polegający na naruszeniu ochrony danych osobowych, prowadzący do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, ujawnienia lub nieuprawnionego dostępu do danych osobowych, stanowi naruszenie bezpieczeństwa danych osobowych.
2. W przypadku stwierdzenia incydentu pracownik jest zobowiązany do zabezpieczenia miejsca zdarzenia i niezwłocznego poinformowania przełożonego oraz inspektora ochrony danych.
3. Inspektor ochrony danych we współpracy z LASI przygotowuje raport i przekazuje go rektorowi wraz z propozycją postępowania w zaistniałej sytuacji. Rektor podejmuje decyzję o dalszym przebiegu postępowania.
4. Jeżeli zgodnie z decyzją rektora incydent z dużym prawdopodobieństwem może skutkować naruszaniem praw i wolności osób fizycznych, których dane dotyczą, zgłasza ten fakt, nie później niż w ciągu 72 godzin po stwierdzeniu naruszenia, Prezesowi Urzędu Ochrony Danych Osobowych, zachowując formę przewidzianą w art. 33 ogólnego rozporządzenia o ochronie danych oraz, jeżeli jest to możliwie, zawiadamia osoby, których dane dotyczą.
5. Użytkownicy systemu informatycznego są zobowiązani do poinformowania ASI lub LASI o każdym przypadku niewłaściwego funkcjonowania systemu informatycznego. W przypadku wadliwego działania systemu informatycznego użytkowników obowiązuje całkowity zakaz wykonywania jakichkolwiek napraw.

Do diagnozowania usterki lub wadliwego działania systemu informatycznego upoważniony jest tylko administrator właściwy dla danego systemu informatycznego lub inna osoba wskazana przez rektora. Jeżeli zachodzi podejrzenie, że wadliwe działanie systemu informatycznego miało wpływ na bezpieczeństwo danych osobowych, ASI lub LASI informuje o tym fakcie inspektora ochrony danych.

6. Rektor lub inspektor ochrony danych mogą wydać polecenie zabezpieczenia komputera pracownika Uczelni w celu dokonania szczegółowego badania.
7. W przypadku naruszenia danych osobowych powierzonych Uczelni przez podmioty zewnętrzne należy wykonać wszystkie czynności zawarte w ust. 2 i 3. Ponadto należy zawiadomić podmiot, który powierzył dane osobowe, o fakcie wystąpienia naruszenia oraz podjętych krokach w celu wyjaśnienia zdarzenia i zminimalizowania jego skutków, co umożliwi realizację odpowiednich działań przez powierzającego. Zgłoszenie powinno nastąpić bez zbędnej zwłoki, nie później jednak niż w ciągu 24 godzin od stwierdzenia naruszenia.

Zadania i odpowiedzialności osób biorących udział w przetwarzaniu danych osobowych

§ 13

1. Administrator danych osobowych (ADO):
   1) analizuje ryzyko nie rzadziej niż raz w roku lub po każdym zdarzeniu mogącym mieć wpływ na bezpieczeństwo danych osobowych,
   2) wdraża odpowiednie środki techniczne i organizacyjne, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób, których dane przetwarza, aby przetwarzanie było zgodne z przepisami prawa i aby móc to wykazać,
   3) powołuje inspektora ochrony danych i jego zastępcę,
   4) wydaje polecenia i upoważnienia do przetwarzania danych osobowych,
   5) zapewnia, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
2. Inspektor ochrony danych (IOD):
   1) uczestniczy we wszystkich sprawach dotyczących ochrony danych osobowych, opiniuje projekty aktualizacji dokumentacji bezpieczeństwa z uwzględnieniem zmian w przepisach prawa,
   2) opiniuje projekty zarządzeń, umów oraz innych dokumentów w zakresie dotyczącym bezpieczeństwa danych osobowych,
   3) monitoruje przestrzeganie Polityki ochrony danych osobowych na Politechnice Śląskiej oraz przepisów prawa w zakresie bezpieczeństwa danych osobowych poprzez wykonywanie audytów i wydawanie rekomendacji,
   4) pełni funkcję punktu kontaktowego dla osób, których dane dotyczą,
   5) pełni funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych,
   6) prowadzi szkolenia dla LPODO,
   7) udziela konsultacji administratorowi danych osobowych oraz pracownikom z zakresu udostępniania i ochrony danych osobowych,
   8) udziela na żądanie rekomendacji co do oceny skutków dla ochrony danych osobowych,
   9) sporządza i przekazuje rektorowi do dnia 31 stycznia każdego roku roczne sprawozdanie z zadań wykonywanych przez siebie i Biuro Bezpieczeństwa Informacji,
   10) prowadzi rejestry, o których mowa w § 3 ust. 1 pkt 1 i 2 Polityki ochrony danych osobowych na Politechnice Śląskiej,
   11) administruje dostępami do aplikacji służącej do zarządzania procesami ochrony danych osobowych RIG.
3. Kierownicy jednostek i komórek organizacyjnych oraz inne osoby posiadające pełnomocnictwo rektora do wydawania upoważnień do przetwarzania danych osobowych:
   1) na podstawie pełnomocnictwa rektora wydają upoważnienia do przetwarzania danych osobowych pracownikom podległym,
   2) nadzorują przetwarzanie danych osobowych wykorzystywanych do realizacji zadań przypisanych jednostce/komórce organizacyjnej lub w ramach realizacji zadań umownych, tak aby były one przetwarzane z zachowaniem przepisów o ochronie danych osobowych,

3) tworzą warunki organizacyjno-techniczne zapewniające bezpieczeństwo danych osobowych.

4. Lokalny pełnomocnik ochrony danych osobowych (LPODO):
   1) wspiera kierownika jednostki/komórki organizacyjnej w wypełnianiu obowiązków wynikających z przepisów o ochronie danych osobowych,
   2) współpracuje z IOD w działaniach mających na celu podnoszenie świadomości osób przetwarzających dane osobowe w zakresie obowiązków spoczywających na nich, a wynikających z ogólnego rozporządzenia o ochronie danych,
   3) informuje BBI o zidentyfikowanych nowych czynnościach przetwarzania danych osobowych,
   4) dokonuje wpisów do rejestru upoważnień,
   5) bierze udział w czynnościach wyjaśniających w przypadku zaistnienia naruszenia ochrony danych osobowych,
   6) przeprowadza szkolenia wstępne dla osób, które otrzymają upoważnienie do przetwarzania danych osobowych.
5. Biuro Bezpieczeństwa Informacji (BBI):
   1) wspiera IOD w realizacji jego zadań,
   2) prowadzi doradztwo w zakresie przygotowania projektów zarządzeń, procedur i innych dokumentów Uczelni w zakresie ich zgodności z przepisami o ochronie danych osobowych,
   3) prowadzi rejestry, o których mowa w § 3 ust. 1 pkt 3, 4 i 6 Polityki ochrony danych osobowych na Politechnice Śląskiej,
   4) sprawuje nadzór nad rejestrem, o którym mowa w § 3 ust. 1 pkt 5,
   5) dokonuje analizy ryzyka dla zidentyfikowanych przetwarzań minimum raz w roku lub w zakresie przetwarzania, w którym nastąpił incydent prowadzący do naruszenia ochrony danych osobowych,
   6) wraz z osobą odpowiedzialną za wdrożenie nowego przetwarzania przeprowadza dla nowego przetwarzania ocenę skutków dla ochrony danych osobowych.
6. Pracownik:
   1) jest zobowiązany do zapoznania się ze wszystkimi procedurami, zarządzeniami i Polityką ochrony danych osobowych na Politechnice Śląskiej wdrożonymi w Uczelni,
   2) przetwarza dane osobowe wyłącznie na polecenie i z upoważnienia administratora danych osobowych,
   3) odpowiada za zabezpieczenie dokumentów oraz sytemu informatycznego w zakresie realizowanych zadań,
   4) jest zobowiązany do zachowania w tajemnicy informacji pozyskanych w związku z wykonywaną pracą oraz przetwarzanymi danymi osobowymi,
   5) bez zgody swojego przełożonego nie może wynosić, przekazywać w jakiejkolwiek formie i w jakikolwiek sposób dokumentów i danych osobowych poza budynki Uczelni oraz osobom spoza Uczelni nieposiadającym upoważnienia do przetwarzania danych osobowych ADO.
   6) zobowiązany jest do natychmiastowego zgłaszania przełożonemu lub IOD wszystkich zauważonych zdarzeń zagrażających bezpieczeństwu danych osobowych.

Analiza ryzyka naruszenia praw i wolności osób, których dane dotyczą

§ 14

1. Dla zidentyfikowanych w Uczelni przetwarzań ujętych w rejestrach, o których mowa w art. 30 ogólnego rozporządzenia o ochronie danych, minimum raz w roku przeprowadza się analizę ryzyka naruszenia praw i wolności osób fizycznych w związku z przetwarzaniem ich danych osobowych.
2. Analizę ryzyka przeprowadza się również każdorazowo dla przetwarzania, w którym stwierdzono incydent lub naruszenie ochrony danych osobowych.
3. Analizę ryzyka przeprowadza BBI.
4. Inspektor ochrony danych opiniuje proces i wyniki analizy ryzyka.
5. Wyniki analizy ryzyka są przedstawiane rektorowi, który wprowadza plan postępowania z ryzykiem.
6. Analiza ryzyka jest podzielona na dwa etapy:

1) w pierwszym etapie oceniane są skutki dla osób, których dane dotyczą, w związku z przetwarzaniem ich danych w ramach każdej czynności przetwarzania. Kryteria oceny obejmują 10 kategorii skutków: uszczerbek fizyczny, szkoda majątkowa lub strata finansowa, utrata kontroli nad własnymi danymi osobowymi, ograniczenie praw, dyskryminacja, kradzież lub fałszowanie tożsamości, naruszenie dobrego imienia, naruszanie poufnych danych osobowych chronionych tajemnicą zawodową, liczba osób, których dane zostały naruszone (skala naruszenia), inne szkody o charakterze gospodarczym lub społecznym. Następnie dla każdego zidentyfikowanego zagrożenia określa się prawdopodobieństwo jego wystąpienia,

2) drugi etap analizy ryzyka polega na oszacowaniu ryzyka dla każdej kombinacji procesu (czynności przetwarzania), zasobu oraz zagrożenia. Przyjętą skalę przedstawiają tabele nr 1 i 2.

Tabela nr 1 Skala ryzyka naruszenia praw i wolności osób, których dane dotyczą

5 Bardzo wysokie	**Powaga konsekwencji**	5	10	15	20	25
4 Wysokie		4	8	12	16	20
3 Średnie		3	6	9	12	15
2 Niskie		2	4	6	8	10
1 Bardzo niskie		1	2	3	4	5
		Prawdopodobieństwo				

Tabela nr 2 Reakcja na ryzyko i jego ograniczanie

Reakcja na ryzyko i jego ograniczanie		
Poziom istotności		**Działania**
Wysokie ryzyko	15 – 25	Poziom ten oznacza bardzo wysokie ryzyko w rozumieniu motywu 76 ogólnego rozporządzenia o ochronie danych. Poziom ryzyka nieakceptowalny – niezbędne jest niezwłoczne podjęcie działań zaradczych. Proces wymaga stałego monitorowania.
Ryzyko	7 – 14	Poziom ten oznacza ryzyko w rozumieniu motywu 76 ogólnego rozporządzenia o ochronie danych. Poziom ryzyka nieakceptowany – podjęcie działań zaradczych jest niezbędne, może zostać przesunięte w czasie. Proces wymaga okresowego monitorowania.
Niskie ryzyko	4 – 6	Poziom ryzyka akceptowalny – działania są podejmowane w zależności od wymaganych nakładów. Proces wymaga okresowego monitorowania
Bardzo niskie ryzyko/brak	1 – 3	Poziom ryzyka akceptowalny – nie wymaga podejmowania działań.
Metody reakcji na ryzyko		
1. Akceptacja ryzyka 2. Redukcja ryzyka 3. Dzielenie ryzyka 4. Uniknięcie ryzyka		

Ocena skutków dla ochrony danych

§ 15

1. Jeżeli nowy rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, przed rozpoczęciem przetwarzania danych należy dokonać oceny planowanych operacji przetwarzania danych osobowych.
2. Decyzja, czy dana operacja wymaga przeprowadzania oceny dla ochrony danych, jest podejmowana na podstawie analizy następujących okoliczności:
   1) podczas przetwarzania dokonywana będzie ewaluacja lub ocena, w tym profilowanie i przewidywanie (analiza behawioralna), w celach wywołujących negatywne skutki prawne, fizyczne, finansowe lub inne niedogodności dla osób fizycznych,

2) w przetwarzaniu będzie miało miejsce zautomatyzowane podejmowanie decyzji wywołujące skutki prawne, finansowe lub podobne, istotne skutki,
3) w przetwarzaniu będzie miało miejsce systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie, wykorzystujące elementy rozpoznawania cech lub właściwości obiektów, które znajdą się w monitorowanej przestrzeni,
4) przetwarzane będą szczególne kategorie danych osobowych oraz dotyczących wyroków skazujących i czynów zabronionych,
5) przetwarzane będą dane biometryczne wyłącznie w celu identyfikacji osoby fizycznej bądź w celu kontroli dostępu,
6) przetwarzane będą dane genetyczne,
7) dane będą przetwarzane na dużą skalę, gdzie pojęcie dużej skali dotyczy:
   a) liczby osób, których dane są przetwarzane,
   b) zakresu przetwarzania,
   c) okresu przechowywania danych,
   d) geograficznego zakresu przetwarzania,
8) w ramach przetwarzania będzie przeprowadzane porównanie, ocena lub wnioskowanie na podstawie analizy danych pozyskanych z różnych źródeł,
9) przetwarzane będą dane dotyczące osób, których ocena i świadczone im usługi są uzależnione od podmiotów lub osób, które dysponują uprawnieniami nadzorczymi i/lub ocennymi,
10) przy przetwarzaniu danych będą zastosowane innowacyjne rozwiązania technologiczne lub organizacyjne,
11) przetwarzanie samo w sobie uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy,
12) przetwarzane będą dane lokalizacyjne.

3. Jeżeli przetwarzanie wymaga dokonania oceny skutku dla ochrony danych, wówczas obywa się ona z wykorzystaniem oprogramowania RIG. Oceny dokonuje BBI wraz z osobą odpowiedzialną za wdrożenie nowego przetwarzania.
4. Zarówno kwalifikacja do dokonania oceny skutków dla ochrony danych, jak i ewentualna ocena podlegają konsultacji z inspektorem ochrony danych.

Uwzględnienie ochrony danych w fazie projektowania oraz domyślna ochrona danych

§ 16

1. W przypadku opracowywania, projektowania, dokonania wyboru, a także wykorzystywania usług, aplikacji czy innych produktów opierających się na przetwarzaniu danych osobowych niezbędne jest uwzględnienie ochrony danych już w fazie projektowania (privacy by design) oraz domyślnej ochrony danych (privacy by default) przy zastosowaniu odpowiednich środków technicznych i organizacyjnych.
2. Rozwiązania przyjęte w ramach wprowadzanych przedsięwzięć muszą zawierać wbudowane mechanizmy, które pozwolą na przetwarzanie danych osobowych z zachowaniem przepisów o ochronie danych osobowych.
3. Wymogi, o których mowa w ust. 1 i 2, muszą zostać zawarte w specyfikacji warunków zamówienia, zapytaniu ofertowym lub innym dokumencie tego rodzaju.
4. Zapisy, o których mowa w ust. 3, podlegają konsultacji z inspektorem ochrony danych.

Monitoring wizyjny

§ 17

1. Celem zapewnienia bezpieczeństwa pracowników, studentów, doktorantów oraz innych osób przebywających na terenie kampusów Politechniki Śląskiej oraz ochrony mienia stosuje się monitoring wizyjny.
2. Monitoring wizyjny rejestruje obraz, natomiast nie rejestruje dźwięku.
3. Za prawidłowe funkcjonowanie monitoringu oraz zabezpieczanie nagrań odpowiadają zarządcy obiektów lub jednostka wskazana do administrowania monitoringiem.
4. Zarządcy obiektów lub jednostka wskazana do administrowania monitoringiem oznaczają w sposób czytelny i widoczny teren objęty monitoringiem.

5. Monitoring nie może obejmować następujących miejsc:
   1) pomieszczeń udostępnianych organizacjom związkowym,
   2) pomieszczeń socjalnych pracowników,
   3) pomieszczeń sanitarno-epidemiologicznych,
   4) szatni, przebieralni,
   5) stołówek.
6. Zastosowanie monitoringu wizyjnego w pomieszczeniach, o których mowa w ust. 5 pkt 2-5, jest możliwe wyłącznie wtedy, gdy istnieje wysokie prawdopodobieństwo naruszenia bezpieczeństwa osób lub mienia i po uzyskaniu zgody organizacji związkowych działających na Politechnice Śląskiej.
7. Zastosowanie monitoringu w pomieszczeniach, o których mowa w ust. 5 pkt 2-5, nie może naruszać prawa do intymności osób z nich korzystających, zatem zarządca obiektu powinien dopilnować właściwego ustawienia kamer monitoringu.
8. Nagrania obrazu monitoringu wizyjnego przechowuje się nie dłużej niż przez okres 3 miesięcy.
9. W przypadku, w którym nagrania obrazu stanowią dowód w postępowaniu prowadzonym na podstawie prawa lub administrator powziął wiadomość, iż mogą one stanowić dowód w postępowaniu, termin określony w ust. 8 może ulec przedłużeniu do czasu prawomocnego zakończenia postępowania.
10. Wgląd do zarejestrowanego obrazu oraz możliwość uzyskania kopii zapisu mają podmioty, których uprawnienia wynikają bezpośrednio z przepisów prawa (organy ścigania, prokuratura, organy sądownicze).
11. Nagrania mogą być udostępniane innym podmiotom, w tym pracownikom, studentom czy osobom korzystającym z infrastruktury Uczelni, w przypadku zdarzenia bezpośrednio zagrażającego ich bezpieczeństwu i zdrowiu lub mieniu.
12. Udostępnienie nagrań podmiotom, o których mowa w ust. 11, następuje za zgodą rektora, na podstawie pisemnego wniosku złożonego w Biurze Bezpieczeństwa Informacji, którego wzór stanowi załącznik nr 5 do Polityki ochrony danych osobowych na Politechnice Śląskiej.
13. Udostępnienie nagrań z monitoringu wizyjnego nie może naruszać prawa do prywatności osób postronnych będących na nagraniach.
14. Pracownik zabezpieczenia technicznego Straży Akademickiej lub osoba upoważniona przez zarządcę obiektu/kierownika jednostki organizacyjnej – każdy w swoim zakresie działania – prowadzą dziennik systemu wizyjnego, w którym dokumentują:
   1) awarie urządzeń,
   2) udostępnianie wglądu do zapisów monitoringu (imię i nazwisko, jednostka organizacyjna),
   3) wydanie kopii zapisów podmiotom uprawnionym (data wydania, data nagrania, oznaczenie podmiotu, imię i nazwisko osoby odbierającej nośnik, imię i nazwisko osoby wydającej nośnik).
15. Pracodawca informuje pisemnie każdego nowo zatrudnionego pracownika w Uczelni o stosowaniu monitoringu wizyjnego. Informacje tę przekazuje Dział Zasobów Osobowych.

Praca zdalna

§ 18

1. Pracownik, przed podjęciem pracy zdalnej potwierdza, że został przeszkolony z procedur ochrony danych osobowych obowiązujących podczas pracy zdalnej, a wprowadzonych w Uczelni.
2. Wykonując pracę zdalną, pracownik jest zobowiązany do zabezpieczenia danych osobowych (w tym także na nośnikach papierowych) przed osobami postronnymi, w tym wspólnie zamieszkującymi, oraz przed zniszczeniem.
3. Zabronione jest przemieszczanie się z dokumentacją służbową w inne miejsce niż miejsce uzgodnione z pracodawcą na potrzeby wykonywania pracy zdalnej. Zakaz nie dotyczy osób, które otrzymały polecenie wyjazdu służbowego.
4. Zabronione jest przekazywanie dokumentacji papierowej osobom trzecim celem jej dostarczenia do zakładu pracy bez wcześniejszego powiadomienia o tym fakcie pracodawcy oraz otrzymania od niego zgody.
5. Przenosząc dokumentację zawierającą dane osobowe pomiędzy zakładem pracy a miejscem wykonywania pracy zdalnej, należy zastosować odpowiednie środki bezpieczeństwa, polegające w szczególności na

przenoszeniu/przewożeniu dokumentów w zamkniętej teczce. Nie wolno pozostawiać dokumentacji bez nadzoru w miejscach publicznych, ogólnodostępnych.

6. W przypadku korzystania z komputerów lub pamięci przenośnych obowiązkowe jest szyfrowanie danych podczas transportu.
7. Należy używać oprogramowania do szyfrowania wbudowanego w system Windows lub darmowego oprogramowania 7-Zip, lub innego oprogramowania służącego do skutecznego szyfrowania.
8. Po zaprzestaniu pracy zdalnej wszystkie dokumenty wytworzone podczas jej wykonywania pracownik jest zobowiązany przynieść do siedziby pracodawcy, gdzie podlegać będą one bądź archiwizacji, bądź zniszczeniu, zgodnie z jednolitym rzeczowym wykazem akt obowiązującym na Politechnice Śląskiej.
9. Komunikacja pomiędzy zakładem pracy a miejscem wykonywania pracy zdalnej powinna opierać się wyłącznie na bazie służbowej poczty elektronicznej w domenie polsl.pl lub za pośrednictwem dopuszczonego przez administratora danych osobowych oprogramowania.
10. Praca zdalna wymagająca logowania do infrastruktury Politechniki Śląskiej musi odbywać się z wykorzystaniem szyfrowanego połączenia (eduVPN, SSL) lub z wykorzystaniem technologii VDI/VMware.
11. Urządzenie elektroniczne służące do pracy zdalnej musi być wyposażone w aktualny system operacyjny objęty wsparciem producenta.
12. Urządzenie elektroniczne służące do pracy zdalnej musi być wyposażone w aktualny program antywirusowy.
13. Zabrania się pobierania dokumentów/raportów/zestawień zawierających dane osobowe i zapisywania ich na twardych dyskach prywatnego sprzętu wykorzystywanego przez pracownika do pracy zdalnej. W przypadku gdy zaistnieje taka konieczność, po zakończeniu pracy nad sprawą pobrane dokumenty/raport/zestawienia należy usunąć.
14. Pracownik chcący świadczyć pracę zdalną oświadcza, że jest w stanie zapewnić bezpieczne środowisko pracy dla przetwarzania danych osobowych.
15. W przypadku stwierdzenia lub choćby podejrzenia, że podczas pracy zdalnej miało miejsce naruszenie ochrony danych osobowych, pracownik jest zobowiązany do postępowania zgodnie ze wskazaniami § 12 Polityki ochrony danych osobowych na Politechnice Śląskiej.

Gliwice, dnia .....

Pani/Pan*

.....

UPOWAŻNIENIE
do przetwarzania danych osobowych nr .....

Zgodnie z postanowieniami 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) (Dz. Urz. UE L 119 z 04.05.2016) upoważniam[1]

1) Panią/Pana* ..... do przetwarzania danych osobowych w zakresie niezbędnym do wykonywania obowiązków na stanowisku ..... ,

2) Panią/Pana* ..... do przetwarzania danych osobowych w zakresie niezbędnym do wykonywania zadań związanych z ..... (należy wpisać rodzaj zadań)[2].

Upoważnienie obowiązuje od dnia ..... do dnia ...../odwołania*.

Jednocześnie powiadamiam Panią/Pana o obowiązku zachowania w tajemnicy ww. danych oraz obowiązku przestrzegania przepisów ogólnego rozporządzenia o ochronie danych, a także reguł ochrony danych wynikających z „Polityki ochrony danych osobowych na Politechnice Śląskiej" oraz innych procedur bezpieczeństwa informacji.

Upoważnienie obejmuje przetwarzanie danych szczególnych kategorii wydane na podstawie art. 8b ust. 1b ustawy z dnia 4 marca 1994 r. o zakładowym funduszu świadczeń socjalnych.

☐ tak ☐ nie

Upoważnienie obejmuje przetwarzanie danych szczególnych kategorii wydane na podstawie art. 22^{1b} § 3 ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy.

☐ tak ☐ nie

.....
(podpis administratora danych osobowych)

.....
(podpis osoby upoważnianej)

* niewłaściwe skreślić

[1] należy wybrać właściwą opcję
[2] wykonywaniem zadań członka Samorządu Studenckiego/doktoranta/realizacji umowy nr ... itp.

OŚWIADCZENIE
o zachowaniu poufności i zapoznaniu się z przepisami

Ja, niżej podpisana/podpisany* ....., oświadczam, że zobowiązuje się do zachowania w tajemnicy danych osobowych, do których będę miała/miał* dostęp w związku z wykonywaniem obowiązków służbowych/umownych/w związku z pełnioną funkcją*.

Zobowiązuję się przestrzegać zasad i procedur ochrony danych osobowych obowiązujących na Politechnice Śląskiej. Oświadczam, że bez upoważnienia nie będę wykorzystywała/wykorzystywał* danych osobowych przetwarzanych na Politechnice Śląskiej.

Oświadczam, że zostałam poinformowana/zostałem poinformowany* o zasadach dotyczących przetwarzania i zabezpieczenia danych osobowych na Politechnice Śląskiej.

Oświadczam, że zostałam zapoznana/zostałem zapoznany* z przepisami rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dn. 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) oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

Oświadczam, że zostałam poinformowana/zostałem poinformowany* o grożącej mi odpowiedzialności karnej i służbowej.

.....
(podpis osoby składającej oświadczenie)

* niewłaściwe skreślić

Gliwice, dnia .....

Pani/Pan*

.....

COFNIĘCIE UPOWAŻNIENIA
do przetwarzania danych osobowych

Niniejszym informuję, że z dniem ..... cofam Pani/Panu* upoważnienie do przetwarzania danych osobowych nr ..... wydane dnia ..... .

.....
(podpis administratora danych osobowych)

.....
(podpis osoby, której cofane jest upoważnienie)

* niewłaściwe skreślić

ANKIETA
weryfikacyjna podmiotu przetwarzającego

Podmiot powierzający	Nazwa	
	Adres	
	NIP	
	REGON	
	KRS	
Podmiot przetwarzający	Nazwa	
	Adres	
	NIP	
	REGON	
	KRS	
Data		
Imię i nazwisko osoby udzielającej odpowiedzi		

Lp.	Pytanie	Odpowiedź (najlepiej tak/nie)	Uwaga lub uzasadnienie do odpowiedzi
	1. Organizacja		
1.1.	Czy podmiot przetwarzający ma doświadczenie lub wiedzę w zakresie świadczenia usług związanych z przetwarzaniem danych osobowych? Jeśli tak, proszę o opis doświadczenia lub przedstawienie dokumentów potwierdzających posiadaną wiedzę.		
1.2.	Czy podmiot przetwarzający musi wyznaczyć IOD?		
1.3.	Czy podmiot przetwarzający wyznaczył IOD?		
1.4.	Czy IOD posiada odpowiedni poziom wiedzy i doświadczenia?		
1.5.	Czy podmiot przetwarzający ma dział compliance/security?		
1.6.	Czy w przypadku braku wyznaczenia IOD podmiot przetwarzający ma specjalistę z zakresu ochrony danych?		
1.7.	Czy specjalista z zakresu ochrony danych ma odpowiedni poziom wiedzy i doświadczenia?		
1.8.	Czy IOD lub specjalista z zakresu ochrony danych ma odpowiednio wsparcie prawne lub techniczne w zależności od potrzeb?		
1.9.	Czy podmiot przetwarzający gwarantuje, że IOD ma zasoby niezbędne do wykonania zadań, a także zasoby niezbędne do utrzymania jego wiedzy fachowej?		
1.10.	Czy członkowie personelu zostali przeszkoleni i zapoznani z przepisami o ochronie danych osobowych ? Czy jest to udokumentowane? Jeśli tak, proszę wskazać termin ostatniego szkolenia.		
1.11.	Czy członkowie personelu zostali przeszkoleni w zakresie obsługi, w tym bezpiecznego korzystania z systemów i urządzeń informatycznych? Czy jest to		

	udokumentowane? Jeśli tak, proszę wskazać termin ostatniego szkolenia.		
1.12.	Czy członkowie personelu zostali przeszkoleni w zakresie zasad bezpieczeństwa informacji, w szczególności ochrony danych osobowych? Czy jest to udokumentowane? Jeśli tak, proszę wskazać termin ostatniego szkolenia.		
1.13.	Czy podmiot przetwarzający przystąpił i stosuje kodeks postępowania dla swojej branży? Jeśli nie, proszę uzasadnić.		
1.14.	Czy podmiot przetwarzający jest objęty monitorowaniem przestrzegania kodeksu postępowania przez akredytowany podmiot monitorujący?		
1.15.	Czy podmiot przetwarzający ma certyfikat zgodności z RODO zgodnie z przepisami rozporządzenia? Jeśli tak, proszę wskazać wystawcę certyfikatu oraz datę uzyskania.		
1.16.	Czy podmiot przetwarzający zamierza korzystać lub korzysta z usług dalszych podmiotów przetwarzających? Jeśli tak, proszę wskazać, w jakim zakresie oraz udzielić informacji, czy dokonał weryfikacji takich podmiotów, w szczególności, kiedy ostatnio prowadził u nich audyt bezpieczeństwa, w jakiej formie i jaki był wynik audytu.		
	2. Zabezpieczenia		
2.1.	Czy podmiot przetwarzający prowadzi regularne audyty bezpieczeństwa, w szczególności ochrony danych osobowych? Jeśli tak, proszę wskazać datę ostatniego audytu oraz rodzaj wniosków końcowych.		
2.2.	Czy podmiot przetwarzający posiada certyfikaty w zakresie bezpieczeństwa informacji lub wdrożył system zarządzenia bezpieczeństwa informacji? Jeśli tak, proszę wskazać jakie.		
2.3.	Czy, a jeśli tak, to z jakich urządzeń informatycznych (hardware) korzysta podmiot przetwarzający przy przetwarzaniu powierzonych danych? Czy takie urządzenia są zabezpieczone adekwatnie do ryzyka?		
2.4.	W jakich lokalizacjach podmiot przetwarzający przetwarza powierzone dane osobowe? Czy te lokalizacje są zabezpieczone adekwatnie do ryzyka?		
2.5.	Czy podmiot przetwarzający korzysta z rozwiązań chmury obliczeniowej? Jeśli tak, proszę podać, jakiego rodzaju (prywatna/publiczna/hybrydowa) i od jakich dostawców.		
2.6.	Czy podmiot przetwarzający korzysta z systemów informatycznych (software) opartych na modelu rozwiązań chmury obliczeniowej (SAS)? Jeśli tak, proszę podać, jakiego rodzaju jest to oprogramowanie.		
2.7.	Czy podmiot przetwarzający będzie przetwarzał powierzone dane osobowe w formie papierowej? Jeśli tak, to czy te dokumenty będą zabezpieczone adekwatnie do ryzyka?		
2.8.	Czy podmiot przetwarzający wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku związanemu z ich przetwarzaniem?		

3. Incydenty, postępowania organu, decyzje itp.			
3.1.	Czy u podmiotu przetwarzającego doszło w ciągu ostatnich 12 miesięcy do incydentów bezpieczeństwa? Jeśli tak, to jakiej kategorii i jak często (np. zgubienie pendriv'a bez danych osobowych raz w roku albo włamanie bez kradzieży danych dwa razy w roku)?		
3.2.	Czy u podmiotu przetwarzającego doszło w ciągu ostatnich 12 miesięcy do naruszeń ochrony danych osobowych? Jeśli tak, to jakiej kategorii były to naruszenia, w tym, czy podlegały zgłoszeniu do organu nadzorczego (np. zgubienie niezaszyfrowanego laptopa z danymi osobowymi, dwa razy w zeszłym roku, podlegało zgłoszeniu)?		
3.3.	Jeśli na pytanie 3.2. odpowiedź brzmiała „tak", to jakie zostały podjęte kroki w celu zaradzenia naruszeniu, w tym przeciwdziałania podobnym naruszeniom w przyszłości?		
3.4.	Czy wobec podmiotu przetwarzającego prowadzona była kontrola Prezesa Urzędu Ochrony Danych Osobowych? Jeśli tak, to kiedy i jaki był jej wynik?		
3.5.	Czy wobec podmiotu przetwarzającego było prowadzone postępowanie Prezesa Urzędu Ochrony Danych Osobowych na skutek skargi podmiotu danych? Jeśli tak, to kiedy postępowanie było prowadzone, co było przedmiotem skargi i jaki był wynik postępowania?		
3.6.	Czy podmiot przetwarzający występuje w jakiejkolwiek sprawie sądowej lub sądowo-administracyjnej dot. ochrony danych osobowych? Jeśli tak, to w jakim charakterze, czego dotyczy sprawa oraz jakie jest rozstrzygnięcie?		
4. Przetwarzanie transgraniczne poza EOG			
4.1.	Czy podmiot przetwarzający lub dalszy podmiot przetwarzający, z którego usług korzysta podmiot przetwarzający, przetwarza dane osobowe poza EOG?		
4.2.	Jeśli tak, to w jakim kraju?		
4.3.	Jeśli tak, to na jakiej podstawie dane osobowe są transferowane poza EOG?		
4.4.	Jeśli tak, to w jakim celu?		
4.5.	Jeśli tak, to czy jest to związane z rozwiązaniami technicznymi, np. korzystanie z serwerów?		
4.6.	Jeśli powierzone dane są przetwarzane na terenie krajów, co do których może zostać utracone prawo do transferu danych, to czy podmiot przetwarzający posiada odpowiednią procedurę w celu legalizacji takiego przetwarzania?		
5. Polityki i procedury			
5.1.	Czy podmiot przetwarzający posiada politykę ochrony danych osobowych lub podobną? Jeśli tak, proszę przedstawić potwierdzenie przyjęcia takiej polityki i jej wdrożenia.		
5.2.	Czy podmiot przetwarzający posiada procedury realizacji praw osób, których dane dotyczą oraz spełniania obowiązku informacyjnego? Jeśli tak, proszę przedstawić potwierdzenie przyjęcia takich procedur i ich wdrożenia.		
5.3.	Czy podmiot przetwarzający posiada procedurę postępowania w sprawie		

	naruszenia? Jeśli tak, proszę przedstawić potwierdzenie przyjęcia takiej procedury i jej wdrożenia.		
5.4.	Czy podmiot przetwarzający nadaje upoważnienia do przetwarzania danych osobowych personelowi?		
5.5.	Czy podmiot przetwarzający prowadzi rejestr nadanych upoważnień?		
5.6.	Czy podmiot przetwarzający zobowiązuje personel do zachowania w tajemnicy wszelkich danych osobowych?		
5.7.	Czy podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania?		
5.8.	Czy podmiot przetwarzający przeprowadził analizę ryzyka? Jeśli tak, proszę o załączenie wyników analizy ryzyka dla procesu, który będzie dotyczył powierzonych danych osobowych.		
5.9.	Czy podmiot przetwarzający korzysta z narzędzia wspomagającego zarządzanie bezpieczeństwem danych osobowych? Jeśli tak, to z jakiego?		

ANKIETA
dotycząca umowy powierzenia przetwarzania

1. Okres obowiązywania umowy powierzenia przetwarzania	
2. Kategorie czynności przetwarzania wykonywane w imieniu administratora	
3. Kategorie osób, których dane dotyczą, oraz kategorie danych osobowych	
4. Inne podmioty, którym podmiot przetwarzający będzie podpowierzał dane osobowe	
5. Informacje o ewentualnym przekazywaniu danych do państwa trzeciego	
6. Informacje o administratorze danych osobowych: 1) nazwa administratora, 2) dane kontaktowe, 3) IOD – dane kontaktowe	
7. Szczególne wymagania administratora związane z przetwarzaniem powierzonych przez niego danych	

Wnioskodawca:

.....
(imię i nazwisko)

.....
(nazwa firmy)*

.....
(adres)

.....
(dane kontaktowe)

WNIOSEK
o udostępnienie danych osobowych w postaci
nagrania zapisu obrazu z monitoringu wizyjnego

W związku ze zdarzeniem: .....

.....

.....

.....
(opis zdarzenia)

wnoszę o udostępnienie danych osobowych w postaci nagrania zapisu obrazu z monitoringu wizyjnego w celu:

.....

.....

.....

.....

Szczegóły zdarzenia:

1) dokładna data: .....
(dzień, miesiąc, rok, godzina)
2) miejsce: .....
3) dodatkowe informacje: .....

.....
(data i podpis wnioskodawcy)

* jeżeli dotyczy