Zarządzenie Nr 27/2018

Dyrektora Centrum Materiałów Polimerowych i Węglowych PAN

z dnia 21 listopada 2018

w sprawie wprowadzenia Polityki ochrony danych osobowych w Centrum Materiałów Polimerowych i Węglowych PAN

1. W związku z wejściem w życie 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) wprowadzam Politykę ochrony danych osobowych w Centrum Materiałów Polimerowych i Węglowych PAN, która stanowi załącznik do tego Zarządzenia.

2. Zarządzenie nr 31/2013 z dnia 13.11.2013 wygasa z dniem wejścia w życie niniejszego Zarządzenia.

3. Zarządzenie wchodzi w życie z dniem podpisania.

Dyrektor Centrum

prof. dr hab. Andrzej Dworak

Otrzymują:

Pracownicy Centrum

Polityka ochrony danych osobowych
w Centrum Materiałów Polimerowych i Węglowych PAN

Podstawa prawna

§ 1

Polityka ochrony danych osobowych w Centrum Materiałów Polimerowych i Węglowych PAN zwana dalej „Polityką" została opracowana 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 /Dz. Urz. UE.L nr 119, str.1/, zwanego dalej RODO oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (zwaną dalej ustawą).

Cel Polityki

§ 2

Celem Polityki jest:

1) uzyskanie optymalnej, wprowadzonej na podstawie analizy ryzyka i zgodnej z prawem ochrony danych osobowych przetwarzanych w Centrum Materiałów Polimerowych i Węglowych PAN oraz zabezpieczenie przed dostępem do danych osób nieupoważnionych, na każdym etapie ich przetwarzania,
2) określenie obowiązków pracowników - w zakresie ochrony przetwarzanych danych osobowych,
3) podnoszenie świadomości pracowników w zakresie ochrony przetwarzanych danych osobowych.

Procesy przetwarzania danych osobowych

§ 3

Centrum Materiałów Polimerowych i Węglowych PAN, jako administrator danych osobowych, przetwarza dane osobowe w procesach dotyczących m.in.:

1) zarządzania zasobami ludzkimi (rekrutacja do pracy, zatrudnianie, obsługa kadrowa, działalność socjalna, bezpieczeństwo i higiena pracy),
2) działalności naukowo-badawczej (badania naukowe, współpraca naukowa),
3) obsługi finansowo-księgowej (rachunkowość, rozrachunki z pracownikami, kontrahentami),
4) innych obszarów działalności(działalność w zakresie ZITA, realizacja projektów i inne).

Zastosowanie Polityki

§ 4

1. Politykę bezpieczeństwa stosuje się w szczególności do:
   1) przetwarzania danych osobowych w sposób tradycyjny oraz w systemach informatycznych,
   2) przetwarzania danych osobowych dotyczących m.in. pracowników i ich rodzin, byłych pracowników, uczestników badań naukowych, uczestników konferencji, seminariów, projektów, kontrahentów, doktorantów,
   3) przetwarzania danych osobowych przekazanych lub powierzonych Centrum.
2. Politykę bezpieczeństwa stosują wszystkie osoby upoważnione do przetwarzania danych osobowych w Centrum Materiałów Polimerowych i Węglowych PAN.

Zasady zabezpieczenia danych

§ 5

1. Ochrona danych osobowych realizowana jest poprzez zabezpieczenia techniczne i organizacyjne, rozwiązania informatyczne - proporcjonalne i adekwatne do ryzyka naruszenia bezpieczeństwa danych osobowych przetwarzanych w CMPW PAN.
2. Dane osobowe w CMPW PAN są:
   1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (zgodność z prawem, rzetelność, przejrzystość),
   2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach (*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, a nieprawidłowe w świetle celów ich przetwarzania powinny być 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 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).*

Podstawowe pojęcia

§ 6

Użyte w Polityce bezpieczeństwa określenia oznaczają:

1) **administrator danych osobowych (ADO) –** Centrum Materiałów Polimerowych i Węglowych PAN reprezentowane przez Dyrektora Centrum,
2) **inspektor ochrony danych (IOD) –** osoba powołana przez Administratora Danych Osobowych, nadzorująca przestrzeganie zasad i wymogów ochrony danych osobowych określonych w RODO i przepisach krajowych,
3) **osoba odpowiedzialna za zasoby informatyczne**– osoba wyznaczona przez administratora danych osobowych, odpowiedzialna za funkcjonowanie systemu informatycznego w CMPW PAN;
4) **pełnomocnik ds. ochrony danych osobowych** (**PODO**)– osoba wyznaczona przez Administratora Danych Osobowych, której zadaniem jest wspieranie IOD w nadzorowaniu zasad ochrony danych osobowych oraz podnoszenie poziomu ochrony danych osobowych w dziale,
5) **pracownik** – osoba zatrudniona na podstawie stosunku pracy lub umowy cywilnoprawnej;
6) **użytkownik** –osoba upoważniona przez ADO do przetwarzania danych osobowych,
7) **strona trzecia –**osoba fizyczna lub prawna, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe,
8) **odbiorca danych** – osoba fizyczna lub prawna, organ publiczny, któremu udostępnia się dane osobowe, udostępnienie może nastąpić na podstawie ustawy, umowy powierzenia, itp.
9) **zgoda osoby, której dane dotyczą** – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

10) **dane osobowe** –informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osoba, 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, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
11) **kategorie danych osobowych:**

a) **szczególne kategorie danych osobowych –** rozumie się przez to łącznie: dane genetyczne- dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej; dane biometryczne- dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne; dane dotyczące zdrowia- dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;

b) **dane zwykłe – dane inne niż wymienione w pkt a,**

12) **zbiór danych –** zestaw danych osobowych utrwalony zarówno w formie elektronicznej jak i tradycyjnej (papierowej) uporządkowanych według określonych kryteriów,
13) **rejestr czynności –** dokument, który ujawnia w jakich procesach Centrum Materiałów Polimerowych i Węglowych PAN przetwarza dane osobowe; rejestr uwzględnia m.in. cel przetwarzania, podstawę prawną przetwarzania danych, kategorię (zwykłe, szczególne) i zakres przetwarzanych danych oraz w jaki sposób dane są zabezpieczone, stanowi załącznik nr 4 do niniejszej Polityki;
14) **przetwarzanie danych –** operacja lub zestaw operacji wykonywanych na danych osobowych, w sposób zautomatyzowany lub niezautomatyzowany, takich jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, łączenie, przesyłanie, zmienianie, udostępnianie i usuwanie, niszczenie, itp.,
15) **usuwanie danych** – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
16) **system informatyczny –** zespół współpracujących ze sobą urządzeń, programów i procedur przetwarzania informacji i narzędzi programowych stosowanych w celu przetwarzania danych osobowych,
17) **system tradycyjny –** zespół procedur organizacyjnych związanych z przetwarzaniem informacji oraz wyposażenie i środki trwałe wykorzystywane w celu przetwarzania danych osobowych na papierze,
18) **hasło –** ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika znany jedynie użytkownikowi,
19) **identyfikator użytkownika (login) –** ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
20) **pomieszczenia** –budynki lub pomieszczenia określone przez administratora, w którym są przetwarzane dane osobowe,

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

Ogólne zasady ochrony danych

§ 7

ADO zapewnia ochronę przetwarzanych danych osobowych m.in. poprzez:

1) wdrożenie odpowiednich środków technicznych i organizacyjnych,
2) przegląd i uaktualnienie środków technicznych i organizacyjnych,
3) nadawanie upoważnień do przetwarzania danych osobowych,
4) wyposażenie i dostosowanie zabezpieczeń w pomieszczeniach do procesu przetwarzania i przechowywania danych osobowych,
5) zaznajomienie pracowników z prawnymi oraz pracowniczymi konsekwencjami naruszenia bezpieczeństwa danych,
6) zapewnienie pracownikom szkoleń w zakresie poszerzania wiedzy i świadomości związanej z zabezpieczeniem przetwarzania i gromadzenia danych,
7) powoływanie i odwoływanie IOD,
8) zgłaszanie naruszenia ochrony danych osobowych do organu nadzorczego oraz zawiadamiania o tym osoby, której dane te dotyczą.

§ 8

1. Za wykonywanie obowiązków ADO w zakresie ochrony danych osobowych wynikających z RODO odpowiadają:
   1) inspektor ochrony danych (IOD),
   2) pełnomocnicy ds. ochrony danych osobowych (PODO)
   3) kierownicy działów/pracowni, kierownicy projektów w zakresie ochrony danych przetwarzanych w podległych im działach lub zadaniach.
2. Za zabezpieczenie przetwarzania danych osobowych w systemie informatycznym odpowiada osoba odpowiedzialna za zasoby informatyczne.
3. Pracownik CMPW PAN odpowiada za przestrzeganie zasad ochrony danych osobowych przetwarzanych na zajmowanym stanowisku.
4. Użytkownicy zobowiązani są do zachowania w tajemnicy danych osobowych i sposobów zabezpieczeń pozyskanych w związku z wykonywaniem obowiązków.
5. Dyrektor Centrum powołuje IOD, PODO oraz wyznacza osobę odpowiedzialną za zasoby informatyczne.

Inspektor ochrony danych

§ 9

1. Inspektora ochrony danych powołuje Dyrektor Centrum. IOD odpowiada za nadzór nad funkcjonowaniem i efektywnością procesów prawidłowego przetwarzania danych osobowych w Centrum Materiałów Polimerowych i Węglowych PAN.

2. Do zadań IOD należy w szczególności:
   1) informowanie Dyrektora Centrum oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich wynikających z RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz przepisów wewnętrznych i doradzanie im w tej sprawie,
   2) monitorowanie przestrzegania RODO, innych przepisów Unii i państw członkowskich o ochronie danych oraz przyjętych przez administratora polityk ochrony danych, lub podmiotu przetwarzającego, w tym podział obowiązków,
   3) organizowanie szkoleń osób uczestniczących w operacjach przetwarzania danych osobowych,
   4) przeprowadzanie systematycznych audytów w organizacji, w której został powołany oraz udzielanie na żądanie ADO zaleceń co do oceny skutków dla ochrony danych oraz systematyczne monitorowanie ich realizacji,
   5) współpraca i pełnienie funkcji punktu kontaktowego dla organu nadzorczego w sprawach związanych z przetwarzaniem danych osobowych,
   6) pełnienie funkcji punktu kontaktowego dla osób, których dane przetwarzane są w Centrum Materiałów Polimerowych i Węglowych PAN,
   7) prowadzenie rejestru czynności przetwarzania danych osobowych w Centrum Materiałów Polimerowych i Węglowych PAN (załącznik nr 4),
   8) udzielanie wskazówek ADO dotyczących środków technicznych i organizacyjnych mających zabezpieczyć dane osobowe, przestrzegania prawa przez administratora lub podmiot przetwarzającego dane, sposobu wykazania ryzyka pod kątem źródła, charakteru, prawdopodobieństwa i wagi zagrożenia oraz w oparciu o najlepsze praktyki pozwalające zminimalizować to ryzyko,
   9) informowania ADO o przypadkach naruszenia bezpieczeństwa danych osobowych, prowadzenia postępowań wyjaśniających w przypadku podejrzenia naruszenia i naruszenia bezpieczeństwa danych osobowych, corocznych przeglądów Polityki oraz jej aktualizowania stosownie do potrzeb,
   10) przygotowanie i przekazanie ADO sprawozdania rocznego z funkcjonowania systemu ochrony danych osobowych CMPiW PAN.
3. IOD wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania przy uwzględnieniu charakteru, zakresu, kontekstu i celu przetwarzania.
4. Przy wykonywaniu swoich zadań IOD podlega bezpośrednio Dyrektorowi Centrum.
5. IOD jest zobowiązany do zachowania tajemnicy i poufności przy wykonywaniu swoich zadań.

§ 10

Dyrektor Centrum jest zobowiązany dołożyć szczególnej staranności w celu ochrony praw i interesów osób, których dane osobowe są przetwarzane, a w szczególności, aby dane osobowe były:

1) przetwarzane zgodnie z prawem,
2) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu bez właściwej podstawy prawnej,
3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
4) przechowywane w postaci umożliwiającej identyfikację osób, których dane dotyczą nie dłużej, niż jest to niezbędne do osiągnięcia celu przetworzenia,
5) przetwarzane na podstawie nadanego upoważnienia.

Pełnomocnik ds. ochrony danych osobowych

§ 11

PODO zobowiązany jest w zakresie działu, do:

1) nadzoru zastosowanych zabezpieczeń danych przed ich nieuprawnionym udostępnieniem,
2) współpracy z IOD w zakresie analizy okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych,
3) nadzoru nad wdrożeniem i przestrzeganiem obowiązujących ustaleń w zakresie udostępniania danych osobowych osobom trzecim,
4) współdziałania z osobą odpowiedzialną za zasoby informatyczne w zakresie nadzorowania i dostępu do systemów informatycznych wykorzystywanych do przetwarzania danych osobowych.

Osoba odpowiedzialna za zasoby informatyczne

§ 12

Podstawowym zadaniem osoby odpowiedzialnej za zasoby informatyczne jest współpraca z IOD oraz PODO w zakresie ochrony danych osobowych pod kątem zabezpieczeń informatycznych, w tym:

1) przygotowanie i wdrażanie instrukcji zarządzania systemem informatycznym,
2) kontrolowanie zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych adekwatną do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności kontrolowanie zabezpieczenia danych przed ich przetwarzaniem z naruszeniem RODO - nie rzadziej niż raz na 12 miesięcy,
3) kontrolowanie zapewnienia ciągłości działania systemu, w tym systematyczne wykonywanie kopii zapasowych, przechowywanie ich w miejscu zabezpieczonym przed nieuprawnionym dostępem, modyfikacją, uszkodzeniem lub zniszczeniem,
4) kontrolowanie zapewnienia awaryjnego źródła zasilania oraz zabezpieczenia przed zakłóceniami w sieci zasilającej systemy informatyczne służące do przetwarzania danych osobowych, których nagła przerwa w pracy mogłaby spowodować utratę danych lub naruszenie ich integralności,
5) nadzór nad naprawą oraz likwidacją urządzeń komputerowych,
6) nadzór nad przeglądem i konserwacją systemów informatycznych służących do przetwarzania danych osobowych, w tym m.in. wykorzystywanie jedynie oprogramowania posiadającego wsparcie producenta oraz systematyczne, automatyczne jego aktualizowanie,
7) zabezpieczenie systemów służących do przetwarzania danych osobowych przed działaniem oprogramowania złośliwego, tj. zastosowanie systemu antywirusowego korzystającego z aktualnej bazy wirusów,
8) dostosowanie wszystkich systemów informatycznych służących do przetwarzania danych osobowych , w tym m.in.:
   a) rejestrowanie dla każdego użytkownika odrębnego identyfikatora,
   b) stosowanie właściwych haseł dostępowych,
   c) zapewnienie, że dostęp do systemu informatycznego jest możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia,
   d) zapewnienie, że systemy odnotowują identyfikator użytkownika wprowadzającego dane osobowe do systemu (chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba),

e) zapewnienie, że systemy posiadają możliwość odnotowania informacji o źródle danych w przypadku zbierania danych nie od osoby, której one dotyczą.

9) nadzór nad zabezpieczeniem pomieszczenia serwerowni przed dostępem osób nieuprawnionych,
10) nadzór nad ochroną przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem,
11) nadzorowanie stosowania zasady „czystego ekranu" polegającej na zakazie zapisywania przez użytkowników systemów informatycznych dokumentów zawierających dane osobowe na pulpicie komputera oraz nakazie blokowania stacji roboczej przed każdorazowym odejściem od stanowiska pracy.

Przetwarzanie danych osobowych

§ 13

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie (załącznik nr 1) oraz, które złożyły stosowne oświadczenie (załącznik nr 2).
2. W przypadku podmiotów zewnętrznych powierzenie czynności przetwarzania danych osobowych następuje na podstawie przepisów prawa lub umowy. Przykładowy wzór umowy stanowi załącznik nr 5.
3. Upoważnienia mogą być wydawane bezterminowo lub na czas określony.
4. IOD przekazuje informację o udzielonych upoważnieniach i oświadczeniach, o których mowa w ust. 1 do Działu Obsługi Badań.
5. IOD prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych (załącznik nr 3) wraz z oświadczeniami potwierdzającymi zapoznanie się z obowiązującymi w tym zakresie przepisami.

§ 14

Osoby przetwarzające dane osobowe:

1) mogą przetwarzać dane osobowe wyłącznie w zakresie udzielonego upoważnienia i tylko w celu wykonywania nałożonych na nich obowiązków,
2) muszą zachować w tajemnicy przetwarzane dane osobowe oraz przestrzegać polityki i innych procedur dotyczących ochrony danych osobowych; przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia w Centrum, a także po ustaniu stosunku pracy,
3) zabezpieczają dane przed dostępem osób nieupoważnionych.

§ 15

1. Każdy pracownik przed dopuszczeniem do przetwarzania danych osobowych podlega przeszkoleniu w zakresie ochrony danych osobowych.
2. Za przeprowadzenie szkolenia odpowiada IOD.
3. Zakres szkolenia obejmuje:
   1) zaznajomienie pracownika z przepisami polityki i innymi procedurami obowiązującymi w Centrum Materiałów Polimerowych i Węglowych PAN w zakresie ochrony danych osobowych,
   2) sposoby ochrony danych osobowych przed osobami trzecimi i procedury udostępniania tych danych osobom, których one dotyczą,
   3) obowiązki osób upoważnionych do przetwarzania danych osobowych i innych,
   4) odpowiedzialność za naruszenie obowiązków z zakresu ochrony danych osobowych.

4. Szkolenie zostaje zakończone podpisaniem przez pracownika oświadczenia o zobowiązaniu się do przestrzegania zasad ochrony danych osobowych w CMPW PAN.

§ 16

1. Każdy użytkownik jest zobowiązany zapoznać się treścią niniejszej polityki.
2. Obowiązkiem użytkowników jest:
   1) przestrzegać procedur związanych z otwieraniem i zamykaniem pomieszczeń, a także z wejściem do obszarów przetwarzania danych osobowych osób nieupoważnionych,
   2) informować IOD lub PODO o incydentach w zakresie naruszenia zasad bezpieczeństwa,
   3) uczestniczyć w szkoleniach dotyczących ochrony danych osobowych.
2. Użytkownikom zabrania się:
   1) zapisywania loginu oraz haseł dostępu do systemu sieci, serwisów internetowych oraz innych programów w miejscach, które umożliwiłoby osobom trzecim zapoznanie się z nimi,
   2) udostępniania stanowisk roboczych oraz istniejących na nich danych (w postaci elektronicznej jak i wydruków) osobom nieupoważnionym,
   3) samowolnego instalowania i używania programów komputerowych bez zgody osoby odpowiedzialnej za zasoby informatyczne,
   4) uruchamiania programów otrzymanych pocztą elektroniczną oraz odczytywania listów o wątpliwej treści,
   5) kopiowania całości lub części baz danych zawierających dane osobowe na jakichkolwiek nośnikach bez uprzedniego skanowania nośnika pod kątem zabezpieczeń przed szkodliwym oprogramowaniem.

§ 17

1. Dane osobowe są przetwarzane w rejestrach i kartotekach w formie dokumentów oraz na sprzęcie, urządzeniach i z użyciem oprogramowania - służące do przetwarzania danych w systemach informatycznych.
2. IOD tworzy rejestr czynności przetwarzania danych osobowych - załącznik nr 4.
3. Wykaz obszarów przetwarzania danych osobowych i sposobu ich zabezpieczenia oraz wykaz czynności przetwarzania danych osobowych w działach sporządza IOD wraz z PODO.

Zasady dostępu do pomieszczeń

§ 18

1. W Centrum Materiałów Polimerowych i Węglowych PAN do pomieszczeń, w których są przetwarzane dane osobowe (załącznik nr 7) mają dostęp osoby upoważnione do przetwarzania danych osobowych zgodnie z zakresami upoważnień. Osoby trzecie mogą w nich przebywać tylko w obecności pracownika upoważnionego do przetwarzania danych osobowych. Na portierni prowadzony jest rejestr gości odwiedzających.
2. Klucze do pomieszczeń przechowywane są na portierniach i pobierane przez upoważnione osoby. Pracownik ochrony ewidencjonuje pobranie i odbiór kluczy w książce raportu, której wzór stanowi załącznik nr 9. Wykonywanie kopii kluczy jest niedozwolone.
3. ADO upoważnia Kierownika Działu Obsługi Badań do prowadzenia i aktualizacji listy osób, które mogą pobierać klucze na portierni (załącznik nr 8). Kierownik Działu Obsługi Badań każdorazowo przekazuje aktualną ewidencję pracownikom ochrony (załącznik nr 10).

4. Użytkowników obowiązuje zasada tzw. „polityki czystego biurka", mająca na celu określenie zasad pozostawienia pomieszczeń po zakończeniu pracy.
5. Wszelkie dokumenty znajdujące się na biurku lub w innych łatwo dostępnych miejscach muszą zostać zabezpieczone przed nieuprawnionym dostępem osób trzecich.
6. Hasła, kody, klucze lub inne nośniki informatyczne muszą zostać zabezpieczone przed nieuprawnionym dostępem osób trzecich.
7. Komputery stacjonarne oraz przenośne, po opuszczeniu stanowiska pracy muszą pozostawać wyłączone lub zablokowane.

Zasady udostępniania danych osobowych

§ 19

1. Udostępnianie danych osobowych w celach innych niż włączenie do kartoteki lub zbioru, może nastąpić na pisemny wniosek (załącznik nr 11) chyba, że przepis ustawy stanowi inaczej.
2. Decyzję o udostępnieniu danych osobowych podejmuje ADO.
3. Udostępnianie instytucjom lub osobom spoza Centrum danych osobowych może odbywać się odpowiednio, za pośrednictwem Działu Obsługi Badań po uprzedniej zgodzie IOD lub przez IOD.
4. Udostępnianie danych osobowych funkcjonariuszom właściwych służb (policja, prokuratura) może nastąpić na pisemny wniosek zawierający:
   1) oznaczenie wnioskodawcy,
   2) wskazanie podstawy prawnej,
   3) określenie rodzaju i zakresu potrzebnych informacji oraz formy ich przekazania,
   4) wskazanie imienia, nazwiska i stopnia służbowego osoby upoważnionej do pobrania informacji lub zapoznania się z ich treścią.
5. Ustne udostępnienie danych osobowych może nastąpić tylko w sytuacjach wymagających niezwłocznego działania albo podczas wykonywania czynności mających na celu ratowanie życia i zdrowia ludzkiego lub mienia i wyłącznie po okazaniu legitymacji służbowej przez funkcjonariusza.
6. Należy zażądać pokwitowania pobrania dokumentów lub potwierdzenia wglądu w ich treść.
7. Jeżeli jednak pokwitowanie nie jest możliwe, należy sporządzić notatkę służbową.
8. Właściwe służby, w celu wykonywania czynności operacyjno-rozpoznawczych, mogą przetwarzać dane osobowe, bez wiedzy i zgody osoby, której te dane dotyczą.
9. Prowadzi się rejestr osób, którym udostępniono dane osobowe na wniosek (załącznik nr 12).

Obowiązek informacyjny

§ 20

1. Osoba, której dane dotyczą, jest uprawniona do uzyskania potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:
   1) cele przetwarzania,
   2) kategorie danych osobowych,
   3) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych,
   4) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu,

5) informacje o prawie do żądania od ADO sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczących osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania,
6) informacje o prawie wniesienia skargi do organu nadzorczego,
7) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle,
8) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

2. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach związanych z przekazaniem.
3. Osoba, której dane dotyczą, w konkretnych przypadkach przewidzianych w ustawie ma prawo do:
   1) uzyskania informacji,
   2) dostępu do danych,
   3) usunięcia danych,
   4) przenoszenia lub sprostowania,
   5) ograniczenia przetwarzania,
   6) sprzeciwu.

Powierzenie danych osobowych do przetwarzania

§ 21

1. Podmiotem przetwarzającym może być wyłącznie podmiot, który zapewnia wystarczające gwarancje stosowania odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.
2. Podmiot przetwarzający nie może korzystać z usług innego podmiotu przetwarzającego bez uprzedniej pisemnej zgody ADO (podpowierzenie).
3. Przetwarzanie przez inny podmiot odbywa się na podstawie umowy lub innego dokumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i ADO; określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa ADO. Umowa lub inny dokument prawny stanowią w szczególności, że podmiot przetwarzający:
   1) przetwarza dane osobowe wyłącznie na udokumentowane polecenie ADO – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba, że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje ADO o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny,
   2) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,
   3) podejmuje wszelkie środki bezpiecznego przetwarzania danych osobowych,

4) biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO;
5) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga ADO wywiązać się z obowiązków określonych w art. 32–36 RODO;
6) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji ADO usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;
7) udostępnia ADO wszelkie informacje niezbędne do przeprowadzania audytów, w tym inspekcji, i przyczynia się do nich.

Wdrożone środki zabezpieczenia danych osobowych

§ 22

1. Zabezpieczenia organizacyjne obejmują:
   1) przetwarzanie danych osobowych w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych
   2) analizę ryzyka naruszeń danych osobowych,
   3) wdrożenie polityki ochrony danych osobowych i Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych ,
   4) wyznaczenie IOD ,
   5) procedurę postępowania w sytuacji naruszenia ochrony danych osobowych,
   6) prowadzenie rejestru czynności przetwarzania,
   7) przetwarzanie danych wyłącznie przez osoby posiadające upoważnienia,
   8) zaznajomienie osób zatrudnionych przy przetwarzaniu danych z przepisami dotyczącymi ochrony danych osobowych,
   9) zobowiązanie osób zatrudnionych przy przetwarzaniu danych osobowych do zachowania ich w tajemnicy
   10) przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych,
   11) dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonuje się takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści.
2. Zabezpieczenia techniczne obejmują m.in.:
   1) wewnętrzną sieć komputerową zabezpieczono poprzez odseparowanie od sieci publicznej za pomocą urządzenia HP Proliant DL380 które stanowi bramę internetową z zaporą firewall realizującą filtrację pakietów,
   2) stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową,
   3) komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkowania i cykliczne wymuszanie zmiany hasła,
   4) polityka czystego ekranu,
3. Środki ochrony fizycznej obejmują m.in.:

1) obszar, na którym przetwarzane są dane osobowe, poza godzinami pracy, jest chroniony; zaleca się stosowanie ochrony i monitoringu,
2) urządzenia służące do przetwarzania danych osobowych umieszczone są w zamykanych pomieszczeniach,
3) dokumenty i nośniki informacji zawierające dane osobowe przechowywane są w zamykanych na klucz szafach,
4) polityka czystego biurka.

Bezpieczeństwo informatyczne

§ 23

Programy komputerowe, wykorzystywane do przetwarzania danych osobowych, uruchamiane są na serwerach oraz komputerach osobistych, zlokalizowanych w pomieszczeniach zgłoszonych i ujętych w ewidencji obszarach przetwarzania danych osobowych.

§ 24

Osoba odpowiedzialna za zasoby informatyczne wraz z IOD opracowują zasady:

1) zapewniania awaryjnego zasilania komputerów i innych urządzeń mających wpływ na bezpieczeństwo przetwarzania informacji,
2) korzystania z komputerów przenośnych, w których przetwarzane są dane osobowe, a w szczególności autoryzacji dostępu do zbiorów danych osobowych,
3) nadzoru nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych i nośników na których znajdują się dane osobowe,
4) uwierzytelniania użytkowników w systemach informatycznych - w tym nadawania identyfikatorów i zarządzania hasłami użytkowników oraz częstotliwości zmian haseł, które zawiera instrukcja określająca sposób zarządzania systemami informatycznymi służącymi przetwarzaniu danych osobowych,
5) nadzoru nad sprawdzeniem systemów informatycznych pod kątem obecności nieuprawnionego oprogramowania, wirusów oraz zabezpieczeń przed atakami z sieci,
6) nadzoru nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących przetwarzaniu danych osobowych oraz innymi czynnościami wykonywanymi na zbiorach danych,
7) nadzoru nad systemami komunikacyjnymi w sieci komputerowej oraz przesyłanymi danymi,
8) nadzoru nad obiegiem i przechowywaniem dokumentów zawierających dane osobowe generowane przez systemy informatyczne,
9) podejmowania działań zabezpieczających system informatyczny w przypadku naruszenia jego zabezpieczeń.

Postępowanie w przypadku naruszenia ochrony danych osobowych

§ 25

1. Przed przystąpieniem do pracy użytkownik obowiązany jest dokonać oględzin swojego stanowiska pracy oraz urządzeń komputerowych, w tym zwrócić szczególną uwagę, czy nie zaszły okoliczności wskazujące na naruszenie lub próby naruszenia ochrony danych osobowych przetwarzanych w systemach informatycznych, jak i tradycyjnych.
2. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie IOD oraz osobę odpowiedzialną za systemy informatyczne.

§ 26

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych IOD:

1) ocenia zastałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane oraz stan urządzeń, a także identyfikuje wielkość negatywnych następstw incydentu,
2) wysłuchuje osobę, która zauważyła incydent,
3) zbiera i zabezpiecza dowody,

a dodatkowo wraz z osobą odpowiedzialną za systemy informatyczne:

4) zabezpiecza system przed dalszym rozprzestrzenieniem się zagrożenia,
5) zabezpiecza dane przetwarzane w systemie informatycznym oraz hasła dostępu i inne w celu późniejszej analizy,
6) podejmuje decyzje o dalszym postępowaniu, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych.

§ 27

IOD sporządza raport z przebiegu zdarzenia, w którym powinny się znaleźć w szczególności informacje o:

1) dacie i godzinie powiadomienia,
2) godzinie pojawienia się w pomieszczeniach, w których przetwarzane są dane,
3) sytuacji, jaką zastał,
4) podjętych działaniach wraz z uzasadnieniem.

§ 28

IOD podejmuje kroki zmierzające do likwidacji naruszeń zabezpieczeń danych osobowych i zapobieżenia wystąpieniu ich w przyszłości. W tym celu:

1) w miarę możliwości przywraca stan zgodny z zasadami zabezpieczenia,
2) raportuje przedsięwzięte czynności, wzór raportu stanowi załącznik nr 13.
3) o ile taka potrzeba zachodzi, postuluje wprowadzenie nowych form zabezpieczenia, a w razie ich wprowadzenia nadzoruje zaznajamianie z nimi osób zatrudnionych przy przetwarzaniu danych osobowych.

§ 29

1. W przypadku zaginięcia komputera lub nośników informatycznych, na których były zgromadzone dane osobowe, użytkownik posługujący się komputerem niezwłocznie powiadamia PODO oraz IOD, a w przypadku kradzieży występuje o powiadomienie jednostki policji.
2. W przypadku kradzieży komputera razem z nośnikiem danych, IOD podejmuje działania zmierzające do odzyskania utraconych danych oraz uczestniczy w procesie wyjaśnienia sprawy w organach ścigania.

§ 30

1. W przypadku stwierdzenia naruszenia danych osobowych, gdy istnieje prawdopodobieństwo, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych ADO ma obowiązek:

1) bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia zgłosić naruszenie organowi nadzorczemu; do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia,
2) udokumentować wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze;

2. Zgłoszenie, o którym mowa w pkt 1 zawiera:
   1) opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazuje kategorie i przybliżoną liczbę osób, których dane dotyczą oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
   2) imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
   3) opis możliwych konsekwencji naruszenia ochrony danych osobowych,
   4) opis środków zastosowanych lub proponowanych przez ADO w celu zaradzenia naruszeniu ochrony danych osobowych, w tym podjęte lub zalecane środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

§ 31

1. Procedura opisana w § 30 ma zastosowanie jedynie w przypadku, gdy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.
2. ADO bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o naruszeniu jej danych osobowych.
3. Zawiadomienie następuje w formie pisemnej lub elektronicznej (za pomocą poczty e-mail, wiadomości sms). Wyjątkowo może być udzielone ustnie, po uprzednim wylegitymowaniu osoby, której dane dotyczą.
5. Zawiadomienie, o którym mowa w ust. 2, nie jest wymagane, w następujących przypadkach:
   1) ADO wdrożył odpowiednie techniczne i organizacyjne środki ochrony, i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym tych danych osobowych,
   2) ADO zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
   3) wymagałoby ono niewspółmiernie dużego wysiłku.

Odpowiedzialność użytkownika

§ 32

1. Niezastosowanie się do polityki ochrony danych osobowych w Centrum Materiałów Polimerowych i Węglowych PAN i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie przepisów Kodeksu Pracy.
2. Niezależnie od rozwiązania stosunku pracy osoby nieprzestrzegające przepisów w zakresie ochrony danych osobowych podlegają odpowiedzialności karnej.

Załączniki do Polityki bezpieczeństwa:

1) Upoważnienie do przetwarzania danych osobowych
2) Oświadczenie pracownika o zaznajomieniu się z Polityką bezpieczeństwa danych osobowych
3) Ewidencja osób upoważnionych do przetwarzania danych osobowych
4) Rejestr czynności przetwarzania danych osobowych: a) dla administratora i b) dla procesora
5) Umowa powierzenia danych osobowych – wzór
6) Instrukcja zarządzania systemami informatycznym służącymi do przetwarzania danych osobowych
7) Wykaz pomieszczeń, w których przetwarzane są dane osobowe
8) Upoważnienie dla Kierownika Działu Obsługi Badań (upoważnienie dostępu do kluczy)
9) Wzór książki raportu
10) Ewidencja osób upoważnionych do poboru kluczy
11) wniosek o udostępnienie danych osobowych
12) Rejestr osób, którym udostępnianie są dane osobowe
13) Raport z naruszenia ochrony danych osobowych

Załącznik nr 1

Wzór upoważnienia pracownika do przetwarzania danych osobowych

_____ *data*	**UPOWAŻNIENIE nr __**

Zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), popularnie nazywanego RODO oraz ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych,

upoważniam Pana/Panią:

_____

imię i nazwisko – stanowisko służbowe

do przetwarzania danych osobowych _____ (klientów, kontrahentów, współpracowników, inne itp.) w imieniu Administratora, gromadzonych w _____ (forma przechowywania danych np. papierowa, elektroniczna , kartoteki, programy itp.), w których przetwarzane są wskazane dane osobowe w zakresie _____.

Niniejsze upoważnienie:

1) zostało wydane na czas _____
2) może być w każdym czasie cofnięte,
3) wygasa z dniem rozwiązania lub wygaśnięcia stosunku pracy lub stosunku cywilnoprawnego z upoważnionym pracownikiem.

_____

Administrator

Załącznik nr 2

Wzór oświadczenia pracownika dotyczące znajomości Polityki Bezpieczeństwa Ochrony Danych Osobowych RODO

OŚWIADCZENIE	
Imię i nazwisko	
Stanowisko służbowe	
Nazwa komórki organizacyjnej	

Stwierdzam własnoręcznym podpisem, że zapoznałem/am/ się z Polityką Bezpieczeństwa Ochrony Danych Osobowych (RODO) dla:

- **Centrum Materiałów Polimerowych i Węglowych PAN z siedzibą w Zabrzu**

Jednocześnie, zgodnie z przepisami:

a) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), popularnie nazywane RODO,

b) ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych,

c) aktami wykonawczymi wydanymi w związku z RODO oraz ustawą o ochronie danych osobowych

zobowiązuję się do ochrony przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem, danych osobowych przetwarzanych w:

- **Centrum Materiałów Polimerowych i Węglowych PAN z siedzibą w Zabrzu**

oraz do zachowania ich w tajemnicy w czasie trwania jak i po ustaniu zatrudnienia.
Równocześnie oświadczam, że zostałem/am/ poinformowany/a/ o odpowiedzialności służbowej i karnej związanej z ochroną danych osobowych.

Administrator	data i podpis składającego oświadczenie

Załącznik nr 3

Ewidencja osób upoważnionych do przetwarzania danych osobowych

L.p.	Imię i nazwisko	Data zapoznania się z dokumentem	Stanowisko Funkcja	Typ umowy lub porozumienia			Zakres rzeczowy uprawnienia	Identyfikator w systemie informatycznym	Ramy czasowe	
				Pracownik	Osoba zatrudniona na umowę cywilnoprawną	Praktykant Stażysta			od	do

Załącznik nr

REJESTR CZYNNOŚCI PRZETWARZANIA

Administrator Danych Osobowych:

Inspektor Ochrony Danych:

Lp.	Nazwa zbioru	Czynności przetwarzania danych osobowych	Nazwa programu w którym przetwarzane są dane;	Zakres danych osobowych- jakie dane są przetwarzane w zbiorze	Cel przetwarzania	Podstawa prawna (przepis prawa, klauzula zgody, umowa, interes publiczny)	Opis kategorii osób, których dane dotyczą	Kategoria danych osobowych, przetwarzanych w ramach zbioru (dane „podstawowe" lub „wrażliwe	Lokalizacja miejsca przetwarzania	Odbiorcy, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorcy w państwach trzecich lub w organizacjach międzynarodowych	Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej	Planowany termin usunięcia danych	Opis technicznych i organizacyjnych środków bezpieczeństwa

Wyjaśnienie niektórych pojęć użytych w Rejestrze czynności:

Załącznik nr

REJESTR CZYNNOŚCI PRZETWARZANIA

a) „dane osobowe" oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania **osobie fizycznej** („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, któr można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jede bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

b) „dane wrażliwe" to dane, na które składają się:

- - „dane genetyczne" oznaczające dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjolo lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;

- - „dane biometryczne" oznaczające dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osob fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;

- - „dane dotyczące zdrowia" oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacj o stanie jej zdrowia;

c) „państwo trzecie" – państwo nie należące do Unii Europejskiej

Załącznik nr

REJESTR CZYNNOŚCI PRZETWARZANIA

Funkcja	Nazwa	Dane kontaktowe
Procesor		
Przedstawiciel Procesora		
Inspektor Ochrony Danych		

Lp.	Administrator Danych Osobowych (nazwa i dane kontaktowe)	Przedstawiciel Administratora Danych Osobowych	Nazwa zasobu	Opis struktury-informacja co zawiera ten zasób/zbiór	Nazwa programu w którym przetwarzane są dane	Zakres danych osobowych-jakie dane są przetwarzane w zasobie	Podstawa prawna (przepis prawa, klauzula zgody, umowa, interes publiczny)	Rodzaje czynności przetwarzań – dokonywanych w imieniu każdego z administratorów	Lokalizacja miejsca przetwarzania	Informacja o przekazaniu danych osobowych do państwach trzecich lub organizacji międzynarodowych	Opis technicznych i organizacyjnych środków bezpieczeństwa
1											
2											
3											
4											
5											
6											
7											
8											

Załącznik nr

REJESTR CZYNNOŚCI PRZETWARZANIA

Wyjaśnienie niektórych pojęć użytych w Rejestrze czynności:

a) „dane osobowe" oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania **osobie fizycznej** („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna t osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfik tor internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

b) „dane wrażliwe" to dane, na które składają się:
- „dane genetyczne" oznaczające dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lu zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;
- „dane biometryczne" oznaczające dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizyczn oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;
- „dane dotyczące zdrowia" oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stan jej zdrowia;

c) „państwo trzecie" – państwo nie należące do Unii Europejskiej

UMOWA
POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Zawarta w dniu _____ w Zabrzu pomiędzy:

1. Instytutem pn.: Centrum Materiałów Polimerowych i Węglowych PAN, ul. Marii Curie-Skłodowskiej 34, 41-819 Zabrze, reprezentowanym przez:
   Dyrektora Centrum – Prof. Andrzeja Dworaka
   zwanym dalej **Zleceniodawcą,**

a

1. _____, prowadzącym działalność gospodarczą pod firmą _____ z siedzibą w _____ przy ul. _____, wpisaną do Centralnej Ewidencji i Informacji o Działalności Gospodarczej pod numerem NIP _____, REGON _____,

lub

2. _____ z siedzibą w _____, ul. _____, _ _ -_ _ _ _____, wpisaną do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy _____ w _____, ___ Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS _____, NIP _____, REGON _____, kapitał zakładowy _____ zł, reprezentowaną przez _____ .

zwanym dalej **Zleceniobiorcą,**

niniejszej treści:

§ 1

Zleceniodawca oświadcza, że jest administratorem danych osobowych Centrum Materiałów Polimerowych i Węglowych PAN, ul. Marii Curie-Skłodowskiej 34, 41-819 Zabrze, w rozumieniu Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE – dalej RODO - w stosunku do danych osobowych powierzonych Zleceniobiorcy.

§ 2

1. Zleceniobiorca może przetwarzać dane osobowe przekazane przez Zleceniodawcę wyłącznie w zakresie oraz w celu zgodnym z niniejszą Umową.
2. Kategorie danych osobowych, których dotyczy przetwarzanie to: .....
3. Zleceniobiorca może przetwarzać dane osobowe wyłącznie w zakresie i w celu świadczenia usług ..... Na danych będą wykonywane następujące operacje: przetwarzanie, modyfikowanie, uaktualnianie, uzupełnianie, archiwizowanie, usuwanie danych.
4. Zmiana zakresu oraz celu przetwarzania danych osobowych może zostać dokonana jedynie w drodze zmiany niniejszej Umowy.

§ 3

1. Zleceniobiorca jest zobowiązany do przestrzegania przepisów ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych - dalej u.o.d.o., RODO oraz przepisów wykonawczych.

2. Zleceniobiorca oświadcza, że przed rozpoczęciem przetwarzania danych podejmie środki techniczne i organizacyjne mające na celu zabezpieczenie powierzonych danych osobowych stosownie do obowiązujących przepisów oraz spełni określone w nich wymagania.
3. Zleceniodawca ma prawo do kontroli sposobu wykonywania niniejszej Umowy przez Zleceniobiorcę odnośnie zobowiązań, o których mowa w niniejszym paragrafie. Warunkiem przeprowadzenia kontroli jest zawiadomienie Zleceniobiorcy w terminie nie krótszym niż 1 dzień przed planowanym terminem jej przeprowadzenia.

§ 4

1. Dostęp do powierzonych danych osobowych mogą posiadać tylko osoby, którym Zleceniobiorca nadał upoważnienia. Na żądanie Zleceniodawcy, Zleceniobiorca niezwłocznie udostępni aktualną listę osób upoważnionych do przetwarzania powierzonych mu danych.
2. Zleceniobiorca oświadcza, że każda osoba (np. pracownik etatowy, osoba świadcząca czynności na podstawie umów cywilnoprawnych, inne osoby pracujące na rzecz Zleceniobiorcy), która zostanie dopuszczona do przetwarzania powierzonych przez Zleceniodawcę danych osobowych zostanie zobowiązana do zachowania tych danych w tajemnicy. Tajemnica ta obejmuje również wszelkie informacje dotyczące sposobów zabezpieczenia powierzonych do przetwarzania danych osobowych.

§ 5

1. Zleceniobiorca nie może wykorzystywać danych, które powierzył mu Zleceniodawca do celów innych niż określonych w Umowie o .....
2. Zleceniobiorca w szczególności nie będzie wykorzystywać ani czerpać z powierzonych danych osobowych informacji do celów reklamowych lub innych podobnych celów handlowych. Zleceniodawca zastrzega sobie wszelkie prawa, tytuły prawne i interes prawny do wykorzystania danych osobowych. Zleceniobiorca nie nabywa żadnych praw do danych poza prawami, które Zleceniodawca przyzna Zleceniobiorcy w celu świadczenia usług będących przedmiotem umowy z dnia .....
3. Zleceniobiorca odpowiada za szkody, jakie powstaną wobec Zleceniodawcy lub osób trzecich w wyniku niezgodnego z prawem przetwarzania danych osobowych objętych niniejszą umową.
4. Zleceniobiorca po zakończeniu przetwarzania danych zobowiązany jest do niezwłocznego usunięcia lub zwrotu powierzonych mu danych.
5. Na każde życzenie Zleceniodawcy, Zleceniobiorca ma obowiązek przedstawić w terminie 7 dni pisemny protokół potwierdzający fakt zniszczenia danych osobowych.

§ 6

1. Zleceniodawcy przysługuje prawo kierowania zapytań do Zleceniobiorcy w zakresie prawidłowości wykonania przez Zleceniobiorcę obowiązków dotyczących zabezpieczenia powierzonych mu na podstawie niniejszej Umowy danych.
2. Zleceniobiorca zobowiązuje się udzielić odpowiedzi na zapytanie, o którym mowa w ust. 1, w terminie 24 godzin od daty wpływu zapytania.
3. Zleceniobiorca będzie współpracował ze Zleceniodawcą aktywnie i bez zbędnej zwłoki w taki sposób, aby osoby, których dane dotyczą mogły korzystać z przysługujących im na mocy przepisów o ochronie danych osobowych praw.

§ 7

Jeśli Zleceniobiorca dowie się o jakimkolwiek bezprawnym dostępie do danych Zleceniodawcy, przechowywanych na sprzęcie Zleceniobiorcy lub w obiektach

Zleceniobiorcy lub jakimkolwiek nieautoryzowanym dostępie do takiego sprzętu lub urządzeń, gdzie w każdym z tych przypadków taki dostęp skutkuje utratą, ujawnieniem lub zmianą danych Zleceniodawcy (z których każdy jest "Incydentem Bezpieczeństwa"), Zleceniobiorca niezwłocznie -nie później niż w terminie 24 godzin:

a) powiadomi Zleceniodawcę o Incydencie Bezpieczeństwa;
b) zbada Incydent Bezpieczeństwa i dostarczy Zleceniodawcy szczegółowych informacji o tym Incydencie;
c) podejmie uzasadnione kroki w celu złagodzenia skutków i zminimalizowania wszelkich szkód powstałych w wyniku Incydentu Bezpieczeństwa. Zgłoszenie ewentualnych Incydentów Bezpieczeństwa będzie dostarczane Zleceniodawcy w formie pisemnej, w tym za pośrednictwem poczty elektronicznej.

§ 8

Zleceniobiorca niezwłocznie poinformuje Zleceniodawcę o jakimkolwiek zapytaniu, działaniu, dochodzeniu lub inspekcji prowadzonej przez organy działające w zakresie ochrony danych lub przez organy sądowe w ramach przepisów o ochronie danych osobowych.

§ 9

1. Strony oświadczają, że zawierają niniejszą Umowę na czas trwania umowy o świadczenie usług, przy czym termin jej wypowiedzenia wynosi tydzień.
2. Zleceniodawca ma prawo wypowiedzieć niniejszą Umowę w trybie natychmiastowym, gdy Zleceniobiorca:

a) wykorzystuje dane osobowe rażąco naruszając przepisy o ochronie danych osobowych, na co Zleceniodawca zwróci Zleceniobiorcy uwagę na piśmie, a Zleceniobiorca w wyznaczonych przez Zleceniodawcę terminie nie usunie wskazanych naruszeń,
b) niezaprzestanie rażącego naruszania przepisów o ochronie danych osobowych, na co Zleceniodawca zwróci Zleceniobiorcy uwagę na piśmie, a Zleceniobiorca w wyznaczonych przez Zleceniodawcę terminie nie usunie wskazanych naruszeń.

§ 10

Zmiana niniejszej Umowy może nastąpić tylko w formie pisemnego aneksu.

§ 11

W sprawach nieuregulowanych niniejszą umową mają zastosowania przepisy u.o.d.o., RODO oraz ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny (tj. Dz. U. z 2017 r. poz. 459).

§ 12

Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Zleceniodawca	**Zleceniobiorca**

Załącznik nr 6

Instrukcja

zarządzania systemami informatycznymi do przetwarzania danych osobowych w Centrum Materiałów Polimerowych i Węglowych PAN

Niniejsza instrukcja określa zasady zarządzania wszystkimi systemami informatycznymi, które użytkowane są w Centrum Materiałów Polimerowych i Węglowych PAN, w tym systemami, w których zachodzi przetwarzanie danych osobowych.

Zasady ogólne

Podstawowe systemy informatyczne Centrum Materiałów Polimerowych i Węglowych PAN dostępne są po zalogowaniu dla każdego użytkownika posiadającego aktywne konto w danym systemie informatycznym. Transmisja danych między serwerem, na którym zainstalowany jest system informatyczny a stacją roboczą jest szyfrowana certyfikatami SHA 256 RSA.

Zasady bezpieczeństwa

Poniżej wymieniono zasady postępowania zapewniające bezpieczeństwo przetwarzanych danych.

§ 1

Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień.

1. Każdy użytkownik komputera lub systemów informatycznych, w których są przetwarzane dane osobowe otrzymuje identyfikator oraz hasło pozwalające na załogowanie się do komputera lub systemu informatycznego. Osoba odpowiedzialna za zasoby informatyczne przeszkoli pracowników z nadawania nowego hasła do komputera i systemu informatycznego.
2. O przyznaniu hasła decyduje osoba odpowiedzialna za zasoby informatyczne.
3. Każdy z użytkowników przed dopuszczeniem do używania komputera lub systemów informatycznych, na którym przetwarzane są dane osobowe jest obowiązany do zapoznania się z niniejszą Instrukcją i Polityką bezpieczeństwa i wpisany zostanie do ewidencji osób upoważnionych.
4. Po zakończeniu pracy na komputerze lub systemie informatycznym użytkownik obowiązany jest do wylogowania się.
5. W przypadku awarii, zagubienia hasła lub innych nieprzewidzianych sytuacji zagrażających bezpieczeństwu danych każdy z użytkowników obowiązany jest niezwłocznie powiadomić Inspektora Ochrony Danych oraz osobę odpowiedzialną za zasoby informatyczne.

6. Adres e-mail po byłym pracowniku zostanie usunięty 3 miesiące po ustaniu stosunku pracy. Z chwilą zakończenia stosunku pracy pracownik zobowiązany jest do skontaktowania się z osobami, z którymi pozostawał w służbowych relacjach w celu poinformowania ich o usunięciu adresu e-mail. Na wniosek przełożonego, lecz nie później niż w dniu zakończenia pracy, możliwe jest zachowanie poczty i danych pracownika, który się zwalnia oraz rekonfiguracja serwera poczty tak, aby korespondencja była przekierowana na inny służbowy adres e-mail na serwerze Centrum.

§ 2

Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Użytkownicy powiadamiani są o haśle ze stosownym pouczeniem o poufnym charakterze hasła oraz obowiązku zachowania go w tajemnicy i zakazie ujawnienia go osobom trzecim, w tym innym użytkownikom.
2. Użytkownik obowiązany jest zapamiętać hasło, o którym mowa powyżej i nie zapisywać go w widocznych lub ogólnie dostępnych miejscach – np. na monitorze.
3. Hasło powinno składać się z ciągu co najmniej 8 znaków, zawierającego co najmniej jedną cyfrę i jeden znak specjalny.
4. Hasła są różne dla każdego z użytkowników.

§ 3

Zabezpieczenia danych osobowych przez użytkownika na stacjach roboczych lub w systemach informatycznych

Aby dane osobowe przetwarzane w systemach informatycznych były zabezpieczone prawidłowo, każdy użytkownik systemu informatycznego ma obowiązek stosować się do poniższych zasad:

1. zakazu udostępniania powierzonego Identyfikatora i Hasła innym użytkownikom, a także osobom nieupoważnionym,
2. zakazu pracowania w systemie na koncie innego użytkownika,
3. obowiązku ochrony wprowadzanych danych przez zabezpieczenie ekranu monitora przed wzrokiem nieupoważnionych osób (odpowiednie ustawienie monitora lub założenie filtru prywatyzującego),
4. aktywizacji wygaszacza ekranu - w przypadku dłuższego opuszczenia stanowiska pracy, należy zaktywizować wygaszasz ekranu z opcją ponownego „logowania się" do systemu lub wylogować się z systemu przed opuszczeniem stanowiska pracy,
5. zabezpieczenia systemu po zakończonej pracy - po zakończeniu pracy w systemie należy wylogować się z systemu i zabezpieczyć swoje stanowisko pracy przed dostępem osób nieupoważnionych;
6. zmiany hasła do komputera w odstępach 30 dniowych, hasło powinno składać się z co najmniej 8 znaków

7. ochrony antywirusowej - stacja robocza powinna być obligatoryjnie wyposażona w system antywirusowy, jeżeli tak nie jest lub jeżeli system antywirusowy pokazuje błędy, należy ten fakt zgłosić do osoby odpowiedzialnej za zasoby informatyczne.
8. korzystanie z poczty Centrum – prowadząc mailową korespondencję służbową należy obligatoryjnie korzystać z poczty Centrum, szczególnie przesyłając dane osobowe. Ruch pomiędzy serwerem pocztowym Centrum, a klientem poczty (np. Mozilla Thunderbird lub przeglądarka WWW) jest szyfrowany. W związku z tym załączniki zawierające dane osobowe przesyłane tą drogą nie wymagają dodatkowego szyfrowania,
9. zakazu korzystania w celach służbowych z zewnętrznych skrzynek pocztowych (gmail, onet, wp i innych), w szczególności do przesyłania danych osobowych,
10. zabrania się przekierowań poczty służbowej na zewnętrzne skrzynki prywatne, jak również wprowadzania danych konfiguracyjnych służbowych adresów e-mail do paneli konfiguracyjnych poczty elektronicznej innych dostawców (np. gmail, interia etc), takie postępowanie grozi wyciekiem danych
11. zabrania się korzystać do celów przetwarzania danych z urządzeń prywatnych z uwagi na możliwy brak odpowiednich zabezpieczeń (program antywirusowy) lub obecność złośliwego oprogramowania na takich urządzeniach,
12. w przypadku wystąpienia nieprawidłowości w mechanizmie uwierzytelniania („logowania się" w systemach lub w poczcie elektronicznej) niezwłocznie należy powiadomić o nich osobę odpowiedzialną za systemy informatyczne.
13. Pracownik odpowiada za sposób korzystania z poczty Centrum i systemów informatycznych, dlatego przekazując dane, w szczególności dane osobowe przy wykorzystaniu technologii informatycznych, należy zwrócić szczególną uwagę na to, komu i jakie dane się udostępnia.

§ 4
Zabezpieczenia techniczne i organizacyjne danych osobowych w Centrum Materiałów Polimerowych i Węglowych PAN

1. Budynki Centrum, w których przetwarzane są dane osobowe są wyposażone w następujące zabezpieczenia:

a.alarm PPOŻ,

b.monitoring wizyjny połączony ze stacją monitoringu firmy ochraniającej budynek/alarm antywłamaniowy,

c.bramę wejściową do budynku zamykaną na klucze,

d.drzwi do pomieszczeń wewnątrz budynku zamykane na klucze,

e.procedurę wydawania kluczy do pomieszczeń osobom uprawnionym,

f.portiernię monitorującą osoby wychodzące i wychodzące z budynku.

2. Do zabezpieczeń technicznych i organizacyjnych danych osobowych w pomieszczeniach, w których są one przetwarzane (strefa/obszar przetwarzania danych osobowych) należą:

a. szafy, w których przechowuje się dokumenty papierowe zawierające dane osobowe obligatoryjnie mają być wyposażone w zamki i być zamykane na klucz po zakończonej pracy lub podczas nieobecności osób upoważnionych do przetwarzania danych osobowych,
b. kierownik pracowni/działu określający zasady oraz sposób wydawania kluczy do szaf
c. dostęp do danych osobowych tylko dla osób upoważnionych,
d. osoby trzecie w strefie przetwarzania danych osobowych muszą przebywać zawsze w towarzystwie osób upoważnionych,
e. polityka „czystego biurka" – należy pracować tylko na tych dokumentach zawierających dane osobowe, które są niezbędne w danym momencie, a po zakończonej pracy wszystkie dokumenty zawierające dane osobowe należy zamykać w szafach.

§ 5

Zabezpieczenia urządzeń przenośnych i nośników wymiennych na których przechowywane są dane osobowe

Jedyne urządzenia przenośne, na których mogą znajdować się dane osobowe to:

a. służbowe laptopy,
b. służbowe tablety,
c. służbowe telefony komórkowe,
d. służbowe nośniki USB.

Urządzenia przenośne zawierające dane osobowe powinny być szyfrowane (np. zaszyfrowane nośniki USB, dyski w laptopach). Należy szczególną uwagę zwrócić na ten fakt, gdy zachodzi konieczność wyniesienia urządzenia przenośnego z budynku Centrum.

§ 6

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

1. Pracownicy zobowiązani są do tworzenia kopii zapasowych danych osobowych przechowywanych na stacjach roboczych z częstotliwością raz na tydzień. Kopie takie należy wykonywać na szyfrowanych nośnikach zewnętrznych.
2. Osoba odpowiedzialna za zasoby informatyczne zobowiązana jest do tworzenia kopii baz danych zawierających dane osobowe.
3. Kopie danych osobowych z komputerów pracowników przechowuje się w budynku Centrum w Zabrzu.
4. Dodatkowo na zasadzie synchronizacji plików między stacjami roboczymi a serwerem wykonywana jest jedna kopia danych wybranych katalogów kluczowych stacji roboczych.

§ 7

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

1. Elektroniczne nośniki informacji zawierające dane osobowe są przechowywane w zamkniętych szafkach z zabezpieczeniem przed dostępem osób trzecich.
2. Kopie zapasowe będą niezwłocznie zniszczone po ustaniu użyteczności danych osobowych tam zawartych.
3. Ze zniszczenia kopii zapasowych spisuje się stosowny protokół opatrzony podpisem Inspektora Ochrony Danych i osoby sporządzającej protokół.
4. Kopie przechowuje się przez okres 2 lat, o ile przepisy nie przewidują obowiązku dłuższego przechowywania. Jeśli użyteczność danych ustała przed okresem 2 lat, kopie mogą zostać zniszczone.

§ 8

Sposób zabezpieczenia stacji roboczych przed działalnością szkodliwego oprogramowania

1. Komputery na których przetwarzane są dane osobowe chronione są przed działaniem wirusów komputerowych oprogramowaniem antywirusowym aktualizowanym na bieżąco.
2. W celu przeciwdziałania atakom spowodowanym przez zainfekowane pliki użytkownik jest zobowiązany skanować system co najmniej dwa razy w tygodniu pod kątem obecności w systemie wirusów i innych zagrożeń.
3. W przypadku wykrycia jakiegokolwiek zagrożenia użytkownik niezwłocznie zawiadamia Inspektora Ochrony Danych oraz osobę odpowiedzialną za zasoby informatyczne.

§ 9

Sposób zabezpieczenia systemu poczty elektronicznej oraz baz danych

1. W bazach danych w których przechowywane są dane osobowe, stosuje się pseudonimizację.

2. Wszelka transmisja danych wewnątrz sieci Centrum jest szyfrowana i zabezpieczona.

3. Wszelka transmisja poczty elektronicznej wychodzącej na zewnątrz jest również szyfrowana i zabezpieczona odpowiednimi certyfikatami SHA-256 RSA.

4. Systemy informatyczne są regularnie testowane pod kątem bezpieczeństwa przechowywania i transmisji danych.

5. Konfiguracja serwera pocztowego Centrum stosuje szereg funkcji zabezpieczających przez podszywaniem się (phishing):

   a. SPF (Sender Policy Framework) określający, jakie serwery mają prawo wysyłać pocztę w imieniu naszej domeny i co ma się stać z pocztą, która nie spełnia tego warunku;

   b. DKIM (DomainKeys Identified Mail). Jest to klucz domeny, który po wygenerowaniu jest dołączany do każdej wiadomości wysyłanej z domeny. Pozwala on określić, że wiadomość rzeczywiście pochodzi z domeny nadawcy wiadomości;

c. DMARC (Domain-based Message Authentication, Reporting and Conformance). Jest to wpis, który bazuje na dwóch powyższych i określa zalecaną przez właściciela domeny politykę, która powinna zostać zastosowana w odniesieniu do wiadomości przychodzących jakoby z domeny nadawcy;

§ 10

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

W przypadku przekazania komputerów do serwisu lub naprawy innym podmiotom wszelkie dane osobowe muszą zostać z nich usunięte z poziomu systemu operacyjnego.

§ 11

Sposób realizacji udostępnienia danych

Udostępnianie danych osobowych odbywa się na zasadach określonych w „Polityce bezpieczeństwa".

§ 12

Procedury rozpoczęcia, zawieszenia i zakończenia pracy

Rozpoczęcie pracy na stanowisku roboczym oraz w systemach informatycznych odbywa się po zalogowaniu się użytkownika poprzez wpisanie loginu i hasła. Kwestie blokowania w czasie nieaktywności oraz procedurę wylogowania opisuje par. 3 pkt. 5 i 6.

Załącznik nr 7

Wykaz pomieszczeń, w których przetwarzane są dane osobowe

L.p.	Lokalizacja, adres i numer budynku	Numer i przeznaczenie pomieszczenia	Piętro	Osoby pracujące w pomieszczeniu	Zabezpieczenie pomieszczenia
1.					
2.					

Załącznik nr 8

Zabrze, dnia 15.11.2018 r.

Centrum Materiałów Polimerowych i Węglowych PAN
ul. Marii Curie-Skłodowskiej 34
41-819 Zabrze

UPOWAŻNIENIE DOSTĘPU DO KLUCZY

Upoważniam Barbarę Niśkiewicz, Kierownika Działu Obsługi Badań do prowadzenia (nadawania upoważnień) i aktualizowania listy pt. „Ewidencja osób upoważnionych do poboru kluczy w pomieszczeniu portierni przy ul. M. Curie-Skłodowskiej 34 w Zabrzu", załącznik nr 10 do Polityki.

Jednocześnie proszę o ewidencjonowanie przez portierów każdorazowego poboru kluczy przez uprawnione osoby według załączonego wzoru (załącznik nr 9). Następnie proszę o przekazywanie po zakończonym miesiącu ewidencji za miesiąc poprzedni.

_____
Administrator

Załącznik nr 9

Wzór książki raportu (ewidencji poboru kluczy do pomieszczeń)

L.p.	Data	Nr klucza (nazwa pomieszcze-nia)	Godzina pobra-nia	Potwier-dzenie zwrotu (czytelnie)	Godzina zdania	Podpis zdającego	Uwagi

Załącznik nr 10

Ewidencja osób upoważnionych do poboru kluczy na portierni

L.p.	Imię i nazwisko osoby upoważnionej	Data udzielenia upoważnienia	Data wycofania upoważnienia	Podpis osoby upoważniającej
1.				
2.				
3.				
4.				
5.				
6.				

Załącznik nr 11

Wzór wniosku o udostępnienie danych osobowych

	Wniosek do: *(proszę o określenie Administratora danych osobowych)*
1) _____ 2) _____	
	Wnioskodawca: *(proszę o podanie imienia i nazwiska, ew. nazwy firmy, danych do korespondencji)*
_____ _____ _____	
	Podstawa prawna upoważniająca wnioskodawcę do przetwarzania danych osobowych, jako odbiorcy danych:
1) _____ 2) _____ 3) _____ 4) _____	
	Cel przetwarzania danych:
1) _____ 2) _____ 3) _____ 4) _____	
	Zakres wymaganych danych, jakie mają być udostępnione:
1) _____ 2) _____ 3) _____ 4) _____	
	Inne informacje umożliwiające wyszukiwanie danych w zbiorze:
1) _____ 2) _____ 3) _____ 4) _____	
	Forma doręczenia udostępnienia danych osobowych:

1) _____
2) _____
3) _____
4) _____

Lista załączników do wniosku:

1) _____
2) _____
3) _____
4) _____

_____

data i podpis osoby wnioskującej
lub upoważnionej przez wnioskodawcę

Załącznik nr 12

Rejestr osób, którym udostępnianie są dane osobowe

L.p.	Imię i nazwisko osoby wnioskującej lub upoważnionej przez wnioskodawcę	Data złożenia wniosku	Zbiór danych i dane, o których udostępnienie wnioskował wnioskujący	Decyzja Data i forma udostępnienia

Załącznik nr 13

Wzór raportu naruszenia ochrony danych osobowych

RAPORT

z naruszenia bezpieczeństwa zasad ochrony danych osobowych

CMPW z siedzibą w Zabrzu

	Data:		**Godzina:**	
	Osoba powiadamiająca o zaistniałym zdarzeniu *(imię i nazwisko, stanowisko służbowe, nazwa użytkownika, jeśli występuje)*			
	Lokalizacja zdarzenia *(np. nr pokoju, pomieszczenia, system)*			
	Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące			
	Przyczyny wystąpienia zdarzenia			
	Podjęte działania			

	Skutki zdarzenia

	Postępowanie wyjaśniające

data i podpis sparzającego raport