*Załącznik nr 1 do Polityki Ochrony Danych osobowych w IBM PAN*

**UPOWAŻNIENIE NR …… / 202…**

**do przetwarzania danych osobowych**

Na podstawie art. 29 Ogólnego Rozporządzenia o Ochronie Danych (RODO) upoważniam Pana/Panią\*:

…………………………………….…………………..………………….………………….………………….………………….………………….

*(Imię i nazwisko)*

zatrudnionego/ą lub współpracującego/ą\* w Instytucie Biologii Medycznej Polskiej Akademii Nauk w

…………………………………….…………………..………………….………………….………………….………………….………………….

*(nazwa komórki organizacyjnej Instytutu Biologii Medycznej PAN)*

do przetwarzania danych osobowych, w celach związanych z wykonywaniem obowiązków:

…………………………………….…………………..………………….………………….………………….………………….………………….

*(nazwa stanowiska lub funkcji, z którą wiąże się przetwarzanie danych)*

polegających na:

…………………………………….…………………..………………….………………….………………….………………….………………….

*(rodzaj czynności, operacji, jakich może dokonywać na danych osobowych)*

Polecenie przetwarzania obejmuje dane w następujące dane:

…………………………………….…………………..………………….………………….………………….………………….………………….

*(typ i zakres przetwarzanych danych)*

Niniejsze upoważnienie obejmuje przetwarzanie danych osobowych w formie tradycyjnej i elektronicznej i stanowi polecenie do przetwarzania wyłącznie w wyżej wskazanym zakresie.

Upoważnienie obowiązuje od dnia **………………** i wygasa z chwilą ustania pełnienia przez Pana/Panią obowiązków o jakich mowa powyżej.

*…………………………………………………………………….*

*(pieczęć i podpis administratora)*

Przyjmuję do wiadomości, iż z upoważnienia do przetwarzania danych osobowych wynika zobowiązanie do zachowania w tajemnicy danych objętych zakresem upoważnienia, w trakcie jak również po ustaniu pełnionych obowiązków oraz do zachowania w tajemnicy informacji o ich zabezpieczeniu.

Zobowiązuje się przetwarzać dane wyłącznie w zakresie wynikającym z upoważnienia i w sposób zapewniający ochronę i bezpieczeństwo danych osobowych, zgodnie z wytycznymi administratora oraz zwrócić dane i zasoby nie później niż z chwilą zakończenia pełnienia obowiązków.

*…………………………………………………………………….*

*(data i podpis osoby upoważnionej)*\*-niepotrzebne skreślić

*Załącznik nr 2 do Polityki Ochrony Danych osobowych w IBM PAN*

**Rejestr upoważnień do przetwarzania danych w IBM PAN**

| **Nr** | **Imię i nazwisko** | **Nazwa stanowiska/ dział** | **Data nadania i podstawa** | **Zakres upoważnienia**  **(zakres danych, czynności)** | **Data ustania i podstawa** |
| --- | --- | --- | --- | --- | --- |
| 1 | Jan Kowalski | Pracownik administracyjny w Dziale Kadr | 01.01.2024 (rozpoczęcie zatrudnienia) | Wszelkie czynności przetwarzania z wyłączeniem usuwania i anonimizacji danych kategorii: pracownicy, kontrahenci, korespondencja - typ: imię, nazwisko, adres korespondencji, pracodawca | 01.03.2024 (zakończenie zatrudnienia) |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

*Instrukcja wypełniania:*

1. *Numer - numer porządkowy upoważnienia zgodny z danymi na upoważnieniu*
2. *Imię i nazwisko - dane osoby upoważnianej*
3. *Nazwa stanowiska/ funkcja - określenie stanowiska i jego położenia w strukturze IBM, jeśli niezależne stanowisko należy to wskazać zamiast danych działu*
4. *Data nadania i podstawa - data nadania upoważnienia (najpóźniej z dniem rozpoczęcia współpracy lub udzielenia dostępu do danych, jeśli udzielenie dostęp nastąpiło z późniejszą datą niż zatrudnienie, np. ze względu na poszerzenie obowiązków) oraz podstawa udzielenie upoważnienia (np. rozpoczęcie zatrudnienia / realizacji zlecenia / czasowa zmiana obowiązków itp.)*
5. *Zakres upoważnienia - określenie w jakim zakresie upoważniony może przetwarzać dane zarówno jak chodzi o typ operacji (wprowadzanie danych, tylko przeglądanie, całość operacji, w tym usuwanie i anonimizowanie, kasowanie z systemu, itp.), jak i kategorie (czyje dane: pracownicy, kontrahenci, dane innych interesariuszy) i typ danych (imię, nazwisko, PESEL, adres e-mail, telefon, itd)*
6. *Data ustania i podstawa - określenie daty kiedy upoważnienie zostało wycofane - z tą datą należy dokonać*

*Załącznik nr 3 do Polityki Ochrony Danych osobowych w IBM PAN*

**Umowa powierzenia przetwarzania danych osobowych**

(dalej „**Umowa powierzenia**”)

zawarta dnia \_\_\_\_\_\_\_\_\_\_\_\_ pomiędzy:

**Instytutem Biologii Medycznej Polskiej Akademii Nauk** z siedzibą w Łodzi, przy ul. Lodowej 106 (93-232 Łódź), NIP: 982-03-52-085, wpisanym do rejestru instytutów naukowych PAN nr RIN - VI - 64/08, reprezentowanym przez:

prof. Jarosława Dziadka - Dyrektora Instytutu

zwaną dalej **„Administratorem danych**” lub „**Administratorem**”,

**Panią/Panem\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** prowadzącą/ym działalność gospodarczą pod firmą \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, z siedzibą w \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, przy ul. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, zarejestrowanym w CEIDG, posiadającym NIP: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_; REGON: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

albo

spółką \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ z siedzibą w \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ przy ul. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, zarejestrowaną w Krajowym Rejestrze Sądowym przez Sąd \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ pod numerem KRS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, posiadającą NIP: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, REGON: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, reprezentowaną przez: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

zwaną dalej **„Podmiotem przetwarzającym”** lub „**Procesorem**”

zwane łącznie dalej „**Stronami**”, a każdy z osobna „**Stroną**”.

**Zważywszy, że**:

1. Strony łączy umowa ramowa o \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ z dnia \_\_\_\_\_\_\_\_\_\_\_, na mocy której Administrator zlecił Procesorowi \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ („**Umowa główna**”),
2. w celu prawidłowego wykonania Umowy głównej niezbędne jest powierzenie przez Administratora do przetwarzania Podmiotowi przetwarzającemu określonych danych osobowych, w trybie art. 28 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)(dalej „**Rozporządzenie**”);
3. Umowa powierzenia ma charakter akcesoryjny wobec Umowy głównej i reguluje wzajemny stosunek Stron i obowiązki w zakresie przetwarzania danych osobowych wynikających z Umowy głównej,

Strony zawierają Umowę powierzenia przetwarzania danych osobowych o następującej treści:

**§ 1**

**Powierzenie przetwarzania danych osobowych**

1. Administrator danych oświadcza, że jest administratorem danych osobowych następującej / następujących kategorii osób: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
2. W celu prawidłowej realizacji przedmiotu Umowy głównej Administrator powierza Podmiotowi przetwarzającemu następujące typy danych osobowych dotyczących kategorii osób wskazanych w ust. 1 powyżej:  
   kategoria: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ; typ danych osobowych: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (dalej „**Dane osobowe**”).
3. Cel i zakres powierzenia przetwarzania Danych osobowych wynika bezpośrednio i ogranicza się do zadań lub usług wynikających z Umowy głównej. Procesor uprawniony jest, w szczególności do dokonywania następujących operacji przetwarzania Danych osobowych: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
4. Powierzone Dane osobowe przetwarzane będą przez Podmiot przetwarzający w formie pisemnej lub elektronicznej.
5. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu Dane osobowe zgodnie z Umową powierzenia, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
6. Podmiot przetwarzający oświadcza, iż stosuje odpowiednie środki techniczne i organizacyjne w rozumieniu Rozporządzenia, które zapewniają bezpieczeństwo powierzonych do przetwarzania Danych osobowych.
7. Podmiot przetwarzający oświadcza, że powierzone mu do przetwarzania Dane osobowe przetwarzane będą wyłącznie na terytorium Unii Europejskiej lub Europejskiego Obszaru Gospodarczego.

**§ 2**

**Obowiązki Procesora**

1. Podmiot przetwarzający oświadcza, że nie powołał Inspektora Ochrony Danych i obowiązki wynikające z umowy realizuje samodzielnie.
2. Podmiot przetwarzający zapewnia, że wdrożył odpowiednie środki techniczne i organizacyjne zapewniające adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem powierzonych mu Danych osobowych, o których mowa w art. 32 Rozporządzenia.
3. Podmiot przetwarzający zobowiązuje się do regularnej weryfikacji i aktualizacji stosowanych przez niego środków technicznych i organizacyjnych tak, aby zapewnić powierzonym Danym osobowym adekwatny stopień ochrony. Podmiot przetwarzający, na każde żądanie Administratora danych, przekaże informacje o stosowanych przez niego środkach organizacyjnych i technicznych związanych z przetwarzaniem Danych osobowych.
4. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych Danych osobowych.
5. Podmiot przetwarzający zobowiązuje się, że jego pracownicy lub współpracownicy (jeśli korzysta), którzy będą przetwarzać Dane osobowe w związku z Umową powierzenia, będą działać na podstawie wyraźnego upoważnienia do przetwarzania danych osobowych, w granicach określonych niniejszą Umową powierzenia oraz że zostaną dopuszczeni do przetwarzania Danych osobowych jedynie po odbyciu szkoleń z zakresu ochrony danych osobowych (w szczególności z ochrony danych osobowych i odpowiedzialności za ochronę tych danych przed niepowołanym dostępem, nieuzasadnioną modyfikacją, zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem danych osobowych). Podmiot przetwarzający oświadcza, że dostęp do Danych osobowych będą miały jedynie osoby, dla których dostęp ten jest niezbędny do wykonania usług określonych w Umowie głównej.
6. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy (o której mowa w art. 28 ust. 3 pkt b Rozporządzenia) przetwarzanych Danych osobowych przez osoby, które upoważni do przetwarzania Danych osobowych w celu realizacji Umowy powierzenia, zarówno w trakcie ich zatrudnienia w Podmiocie przetwarzającym, jak i po jego ustaniu. Podmiot przetwarzając zapewnia, że osoby, które upoważni do przetwarzania Danych osobowych zostaną zobowiązane do zachowania tajemnicy.
7. Podmiot przetwarzający zobowiązuje się wspierać Administratora danych, także przez stosowanie odpowiednich środków technicznych i organizacyjnych, przy spełnieniu żądań osób, których Dane osobowe – powierzone do przetwarzania Procesorowi – dotyczą, a które związane są z realizacją praw osób fizycznych określonych w Rozporządzeniu. Podmiot przetwarzający zobowiązuje się wspierać i współdziałać z Administratorem danych w taki sposób, aby żądanie osoby fizycznej zostało spełnione w terminie określonym w Rozporządzeniu. W szczególności Podmiot przetwarzający zobowiązany jest do udzielenia Administratorowi stosownych informacji lub przekazania niezbędnych dokumentów związanych z żądaniem osoby fizycznej i przetwarzanymi przez niego Danymi osobowymi, nie później niż w terminie 7 dni od dnia skierowania stosownego żądania przez Administratora danych oraz wsparcia w zakresie technicznym przy realizacji żądania osoby fizycznej – nie później niż w terminie 7 dni od dnia otrzymania stosownego żądania od Administratora danych.
8. Podmiot przetwarzający zobowiązuje się współpracować i udzielać wszelkiej pomocy Administratorowi w celu wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia. W szczególności Podmiot przetwarzający będzie udzielał Administratorowi wszelkich informacji dotyczących stosowanych środków bezpieczeństwa, certyfikacji w określonych obszarach, zidentyfikowanych po stronie Podmiotu przetwarzającego ryzyk związanych z przetwarzaniem Danych osobowych oraz wspierał Administratora przy przeprowadzaniu analizy ryzyka lub oceny skutków dla ochrony danych poprzez udzielanie Administratorowi niezbędnych informacji odnośnie przetwarzania Danych osobowych przez Podmiot przetwarzający potrzebnych do przeprowadzenia przez Administratora analizy ryzyka lub oceny skutków dla ochrony danych.
9. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem Danych osobowych na podstawie Umowy głównej, nie później niż w terminie 7 dni zwróci Administratorowi danych wszelkie powierzone mu Dane osobowe i usunie wszelkie ich istniejące kopie lub dokona ich zniszczenia – adekwatnie do woli Administratora, chyba że prawo Unii lub prawo Państwa Członkowskiego nakazują przechowywanie danych osobowych. Przez usunięcie Danych osobowych, rozumieć należy zniszczenie tych danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą (anonimizacja danych). Administrator danych może w każdym przypadku zweryfikować u Procesora wypełnienie obowiązku usunięcia Danych osobowych. W przypadku dalszego powierzenia do przetwarzania Danych osobowych przez Podmiot przetwarzający, na zasadach określonych w § 4 poniżej, Podmiot przetwarzający zapewni, że wszystkie dalsze podmioty przetwarzające usuną lub zanonimizują Dane osobowe na zasadach określonych w niniejszym postanowieniu.

**§ 3**

**Prawo nadzoru i kontroli**

1. Administrator danych jest uprawniony do kontrolowania Podmiotu przetwarzającego w zakresie przetwarzania Danych osobowych pod względem zgodności z postanowieniami Umowy powierzenia i przepisów Rozporządzenia.
2. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i za minimum 3-dniowym uprzedzeniem.
3. Podmiot przetwarzający będzie w pełni współpracował z Administratorem danych podczas kontroli. Podmiot przetwarzający, w szczególności:  
   a. zapewni dostęp do obszarów przetwarzania Danych osobowych oraz dostęp do systemów informatycznych, w których przetwarzane są Dane osobowe;  
   b. umożliwi przeprowadzenie wszelkich czynności kontrolnych w celu oceny zgodności przetwarzania Danych osobowych z obowiązującymi przepisami oraz oceny stosowanych zabezpieczeń (technicznych i organizacyjnych) zapewniających ochronę Danych osobowych;  
   c. udostępni wszelkie niezbędne do przeprowadzenia kontroli dokumenty oraz udzieli wyjaśnień;  
   d. umożliwi przeprowadzenie rozmów z pracownikami (współpracownikami) Procesora przetwarzającymi Dane osobowe, itp.
4. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych, nie dłuższym niż 7 dni po pisemnym żądaniu Administratora.
5. Administrator, w ramach czynności nadzorczych, jest uprawniony do żądania od Podmiotu przetwarzającego, udzielenia informacji związanych z przetwarzaniem Danych osobowych oraz wypełnienia przez Podmiot przetwarzający obowiązków wynikających z niniejszej Umowy powierzenia lub Rozporządzenia. Podmiot przetwarzający zobowiązany jest udostępnić Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w Umowie powierzenia lub Rozporządzeniu.
6. W ramach czynności nadzorczych i kontrolnych Administrator danych jest uprawniony do wydawania Podmiotowi przetwarzającemu pisemnych poleceń odnośnie sposobu wykonania Umowy powierzenia danych.

**§ 4**

**Dalsze powierzenie danych do przetwarzania**

1. Podmiot przetwarzający może powierzyć Dane osobowe do dalszego przetwarzania podwykonawcom jedynie w celu wykonania Umowy głównej, na co Administrator musi wyrazić uprzednią zgodę.
2. Przekazanie powierzonych Danych osobowych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych, chyba że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo Państwa Członkowskiego, któremu podlega Procesor. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający niezwłocznie poinformuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podmiot przetwarzający gwarantuje, że podwykonawca, o którym mowa w § 5 Umowy powierzenia daje te same gwarancje i spełnia obowiązki, jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie powierzenia.
4. Podmiot przetwarzający odpowiada za działania i zaniechania podwykonawcy jak za własne.

**§ 5**

**Odpowiedzialność Podmiotu przetwarzającego**

1. Podmiot przetwarzający jest odpowiedzialny za szkody wyrządzone Administratorowi, osobie fizycznej, której Dane osobowe dotyczą lub innym osobom trzecim w związku z niewykonaniem lub nienależytym wykonaniem Umowy powierzenia, w szczególności niezgodnym z Umową lub Rozporządzeniem przetwarzaniem Danych osobowych.
2. Odpowiedzialność Procesora wobec Administratora danych obejmuje wszelkie szkody poniesione przez Administratora danych na skutek działań lub zaniechań Procesora na zasadach ogólnych przepisów Rozporządzenia lub przepisów Kodeksu cywilnego.
3. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie Danych osobowych niezgodnie z treścią Umowy powierzenia.
4. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, czynnościach sprawdzających, zapytaniach, żądaniach osób których Dane osobowe dotyczą, w szczególności o postępowaniu administracyjnym lub sądowym dotyczącym przetwarzania przez Procesora Danych osobowych określonych w Umowie powierzenia, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.
5. Jeżeli w związku z naruszeniem przepisów Rozporządzania lub Umowy powierzenia przez Procesora Administrator danych zostanie obciążony karą administracyjną lub zobowiązany do wypłaty odszkodowania, Podmiot przetwarzający zobowiązuje się do pokrycia Administratorowi wszelkiej poniesionej z tego tytułu szkody.

**§ 6**

**Czas obowiązywania umowy powierzenia**

Niniejsza Umowa powierzenia zostaje zawarta na czas realizacji Umowy głównej.

**§ 7**

**Zasady zachowania poufności**

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i Danych osobowych otrzymanych od Administratora danych i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („**Informacje poufne**”).
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy Informacji poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy powierzenia, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy powierzenia.
3. Obowiązek zachowania poufności Informacji poufnych obowiązuje przez okres obowiązywania Umowy powierzenia oraz po jej rozwiązaniu lub wygaśnięciu (bez względu na podstawę prawną) przez kolejnych 5 lat.

**§ 8**

**Naruszenie ochrony Danych osobowych**

1. W przypadku stwierdzenia jakiejkolwiek sytuacji stanowiącej naruszenie ochrony Danych osobowych Podmiot przetwarzający zobowiązany jest:
2. niezwłocznie, lecz nie później niż w ciągu 24 godzin od stwierdzenia naruszenia, poinformować o tym Administratora, a informacja będzie zawierać: (1) opis okoliczności i charakteru zdarzenia stanowiącego naruszenie ochrony Danych osobowych oraz jego ustalonych lub podejrzewanych przyczyn; (2) wskazanie kategorii i przybliżonej liczby osób, których Dane osobowe dotyczą; (3) opis możliwych konsekwencji naruszenia ochrony Danych osobowych; (4) opis zastosowanych przez Podmiot przetwarzający środków zaradczych w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony Danych osobowych,
3. podjąć niezwłocznie wszelkie czynności mające na celu usunięcie naruszenia i zabezpieczenie Danych osobowych w sposób należyty przed dalszymi naruszeniami,
4. zebrać wszystkie możliwe dane i dokumenty, które mogą pomóc w ustaleniu okoliczności naruszenia i przeciwdziałaniu podobnym naruszeniom w przyszłości,
5. udzielać Administratorowi wszelkich wyjaśnień.
6. Jeżeli w następstwie naruszenia ochrony Danych osobowych z przyczyn leżących po stronie Podmiotu przetwarzającego, Administrator zostanie obciążony karą administracyjną lub zobowiązany do wypłaty odszkodowania, Podmiot przetwarzający zobowiązuje się do zwolnienia Administratora z odpowiedzialności i zwrotu wszelkiej poniesionej z tego tytułu szkody.

**§ 9**

**Dane kontaktowe**

1. Ze strony Administratora osobami upoważnionymi i odpowiedzialnymi za nadzór nad realizacją Umowy są:  
   a.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, tel. ……………………, email: ………………………….  
   b. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, tel. ……………………, email: …………………………..przy czym dla skuteczności powyższych czynności wystarczy działanie jednej z ww. osób.
2. Ze strony Podmiotu przetwarzającego nadzór nad prawidłową realizacją Umowy powierzenia pełni a.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, tel. ……………………, email: ………………………….
3. Wszelka zmiana wskazanych powyżej osób dla swojej skuteczności będzie wymagała jedynie jednostronnego pisemnego oświadczenia skierowanego do drugiej Strony i nie wymaga dla swej ważności zmiany Umowy powierzenia w formie aneksu i skuteczna będzie od dnia doręczenia drugiej Stronie pisemnego oświadczenia o zmianie
4. Strony postanawiają, że wszelka komunikacja pomiędzy nimi w związku z Umową powierzenia będzie odbywać się przy pomocy środków komunikacji określonych w ust. 1 i 2 powyżej.

**§ 10**

**Postanowienia końcowe**

1. Umowa powierzenia została sporządzona w czterech jednobrzmiących egzemplarzach, po jednym dla każdego z zawierających.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. W wypadku, gdyby któreś z postanowień Umowy powierzenia ew. przyszłych postanowień dołączonych do niniejszej Umowy powierzenia okazało się w całości lub w części nieskuteczne lub niemożliwe do zrealizowania, skuteczność pozostałych postanowień pozostaje nienaruszona. Powyższe dotyczy także ewentualnych luk w uregulowaniach Umowy powierzenia.
4. Wszelkie spory pomiędzy Stronami będą rozstrzygane polubownie. W przypadku braku osiągnięcia porozumienia, ostateczny spór pomiędzy Stronami zostanie rozstrzygnięty przez właściwy sąd powszechny dla siedziby Administratora danych.

**W imieniu Administratora danych**: **W imieniu Podmiotu przetwarzającego**:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Załącznik nr 4 do Polityki Ochrony Danych osobowych w IBM PAN*

**Rejestr umów przetwarzania IBM PAN**

| **Nr** | **Podmiot przetwarzający** | **Dane umowy głównej (numer, przedmiot, data zawarcia)** | **Data zawarcia umowy powierzenia** | **Zakres upoważnienia**  **(zakres danych, czynności)** | **Data rozwiązania umowy** |
| --- | --- | --- | --- | --- | --- |
| 1 | Szkolenia Sp. z o.o. | 23/2024 - Umowa o świadczenie usług szkoleniowych z dnia 01.01.2024 | 01.01.2024 | Wszelkie czynności przetwarzania z wyłączeniem usuwania i anonimizacji danych kategorii: pracownicy, : imię, nazwisko, adres e-amil, stanowisko, pracodawca |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

*Instrukcja wypełniania:*

1. *Numer - numer porządkowy umowy zgodnie z danymi w komparycji umowy*
2. *Podmiot przetwarzający - dane podmiotu lub osoby, której powierzono dane do przetwarzania*
3. *Dane umowy głównej - wskazanie umowy z której wynika zawarcie umowy powierzenia*
4. *Data zawarcia umowy powierzenia - wskazanie daty zawarcia umowy z komparycji*
5. *Zakres upoważnienia - określenie w jakim zakresie podmiot przetwarzający może przetwarzać dane zarówno jak chodzi o typ operacji (wprowadzanie danych, tylko przeglądanie, całość operacji, w tym usuwanie i anonimizowanie, kasowanie z systemu, itp.), jak i kategorie (czyje dane: pracownicy, kontrahenci, dane innych interesariuszy) i typ danych (imię, nazwisko, PESEL, adres e-mail, telefon, itd)*
6. *Data rozwiązania umowy - określenie daty kiedy umowa powierzenia została zakończona*

*Załącznik nr 5 do Polityki Ochrony Danych osobowych w IBM PAN*

**Rejestr czynności przetwarzania IBM PAN**

| **Nazwa czynności przetwarzania** | **Jednostka organizacyjna** | **Cel przetwarzania** | **Kategorie osób** | **Typy danych** | **Żródło danych** |
| --- | --- | --- | --- | --- | --- |
| Rekrutacja pracowników administracyjnych | Dział Kadr | Rekrutacja pracowników | Kandydaci do pracy | Imię, nazwisko, wykształcenie, doświadczenie zawodowe, dane kontaktowe | Kandydat do pracy |
| **Podstawa prawna** | **Planowany termin usunięcia** | **Nawa podmiotu przetwarzającego** | **Kategorie oodbiorców danych** | **Sposób przetwarzania** | **Ogólny opis środków bezpieczeństwa** |
| art. 22(1); zgoda osoby, której dane dotyczą | Do 3 miesięcy od dnia zakończenia rekrutacji | n/d | n/d | w formie tradycyjnej (papierowe akta) oraz elektronicznej w poczcie e-mail oraz folderach kadrowych | Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla osób upoważnionych. |
| **Analiza ryzyka** | **Transfer do kraju trzeciego** |  |  |  |  |
| Po przeprowadzeniu oceny ryzka podjęto decyzję, że ocena skutków dla ochrony danych nie jest wymagana. | n/d |  |  |  |  |

*Instrukcja wypełniania:*

1. *Nazwa czynności przetwarzania - określenie typu czynności, w której przetwarzane są dane,*
2. *Jednostka organizacyjna - wskazanie jednostki organizacyjnej IBM (dział, zespół, niezależne stanowisko) odpowiedzialnej za przetwarzanie w danej czynności*
3. *Cel przetwarzania - odpowiedź na pytanie „po co przetwarzamy dane?” (np. rekrutacja, wypłaty grantów)*
4. *Kategorie osób - odpowiedź na pytanie „czyje dane przetwarzamy?” (np. pracownicy, kontrahenci)*
5. *Typy danych - odpowiedź na pytanie „jakie dane przetwarzamy?” (np. imię, nazwisko, adres)*
6. *Żródło danych - odpowiada na pytanie „skąd mamy dane?” (np. od kandydata, od kontrahenta, od konsorcjanta)*
7. *Podstawa prawna - wskazanie podstawy prawnej z RODO oraz szczególnej podstawy prawnej, jeśli przetwarzanie wynika z obowiązku prawnego (np. art 22(1) KP - dla danych kandydatów w rekrutacji), wskazuje Właściciel danych w porozumieniu z Inspektorem*
8. *Planowany termin usunięcia danych - określenie jak długo musimy lub decydujemy się przechowywać dane albo wskazanie kryteriów decydujących o okresie przetwarzania ()np. 1 rok od daty zakończenia postępowania rekrutacyjnego)*
9. *Nazwa podmiotu przetwarzającego i dane kontaktowe - określenie, czy w procesie bierze udział podmiot przetwarzający oraz wskazanie jego danych;*
10. *Kategorie odbiorców danych - wskazanie czy dane są przekazywane do innych podmiotów z mocy prawa lub umowy innej niż umowa powierzenia, który przetwarza dane we własnym imieniu (np. ZUS, US, towarzystwo ubezpieczeniowe);*
11. *Sposób przetwarzania - wskazanie czy dane są przetwarzane w formie tradycyjnej, czy elektronicznej oraz określenie oprogramowania służącego do przetwarzania - jeśli dotyczy*
12. *Ogólny opis środków bezpieczeństwa - odpowiedź na pytanie „jak dbamy o bezpieczeństwo danych?” (np. zamykane szafki, ograniczony dostęp do pokoi, hasło na komputerze)*
13. *Analiza ryzyka - jeśli dotyczy, analiza ryzyka prowadzona jest odrębnie dla każdego procesu o zidentyfikowanym potencjalnym wysokim ryzyku przez Inspektora,*
14. *Transfer do kraju trzeciego - określenie czy dane są transferowane do kraju trzeciego, ze wskazaniem co to za kraj i w jaki sposób dane są chronione (np. USA, korzystanie z bezpiecznego dostawcy usług)*

*Załącznik nr 6 do Polityki Ochrony Danych osobowych w IBM PAN*

**Regulamin bezpieczeństwa przetwarzania danych osobowych w pomieszczeniach Instytutu**

1. Regulamin obejmuje ogólne wytyczne bezpiecznego postępowania z Danymi osobowymi znajdującymi się w zasobach Instytutu przez Użytkowników.
2. Każdy Użytkownik winien dołożyć należytej staranności w celu zachowania Danych osobowych w poufności, niezależnie od okoliczności i ich opisania w Regulaminie.
3. Użytkownik zobowiązany jest do nadzoru nad zasobami tradycyjnymi oraz starannej pieczy nad powierzonymi kluczami, kartą dostępu, kodem do systemu alarmowego i innymi zabezpieczeniami obowiązującymi w Instytucie.
4. Wszystkie wątpliwości dotyczące bezpieczeństwa Danych osobowych w Instytucie Użytkownik zobowiązany jest zgłosić do Inspektora niezwłocznie po ich powzięciu lub wykryciu.

**Zasady dostępu do budynków i pomieszczeń**

1. W Instytucie obowiązuje system kontrolowanego dostępu do budynków i pomieszczeń za pomocą systemu alarmowego, monitoringu, kart dostępowych i kluczy.
2. Każdej osobie upoważnionej do dostępu do pomieszczeń Instytutu przydzielana jest karta wstępu oraz indywidualny kod dostępowy do systemu alarmowego.
3. Karta wstępu umożliwia wejście do budynku oraz pomieszczeń szatni dla wybranej lokalizacji. Pracownik zobowiązany jest posługiwać się wyłącznie własną kartą i nie wpuszczać ani nie udzielać swojej karty innym osobom.
4. Pracownik może na własną odpowiedzialność wpuszczać zaproszonych przez siebie w celach służbowych gości, pod warunkiem, że od chwili wejścia na teren budynku pozostają oni pod jego stałym nadzorem. Za naruszenie bezpieczeństwa Danych osobowych przez gościa odpowiada Pracownik zapraszający/wpuszczający.
5. Indywidualny kod dostępu umożliwia rozbrojenie i uzbrojenie systemu alarmowego. Zabronione jest ujawnienie przez Pracownika indywidualnego kodu dostępu jakiejkolwiek osobie trzecie, w tym innymi Pracownikowi Instytutu.
6. Pracownik, który jako pierwszy rozpoczyna pracę w danym dniu zobowiązany jest, niezwłocznie po wejściu do budynku, do rozbrojenia systemu alarmowego. Pracownik, który jako ostatni opuszcza budynek w danym dniu zobowiązany jest do uzbrojenia systemu alarmowego.
7. Klucze do poszczególnych pomieszczeń każdy z Pracowników pobiera i zdaje w szatni. Należy pobierać klucze wyłącznie do pomieszczeń do których dostępu Pracownik jest upoważniony, tj. według specyfiki stanowiskowej.
8. Wskazana przez Dyrektora osoba prowadzi wykaz osób upoważnionych do przebywania w poszczególnych pomieszczeniach.
9. Wszystkie pomieszczenia służbowe w budynkach Instytutu po godzinach pracy są zamykane. Za zamknięcie pomieszczenia odpowiada ostatni z Pracowników opuszczający pomieszczenie na koniec dnia pracy.
10. W przypadku opuszczania pomieszczenia, w którym przetwarzane są Dane osobowe, w czasie godzin pracy, Pracownicy zobowiązani są do zamknięcia pomieszczeń i zabrania kluczy. W przypadku opuszczania pomieszczenia na dłuższy czas (np. długie spotkanie, wyjście poza budynek Instytutu) Pracownik zamyka pomieszczenie i zdaje klucz.
11. Za zabezpieczenie oraz bezpieczne przechowanie kluczy do biurek, szaf oraz innych miejsc, gdzie przechowywane są Dane osobowe odpowiada główny Użytkownik lub Właściciel danych. Po zakończeniu pracy z Danymi osobowymi miejsca takie powinny być zamknięte, a klucze do nich przechowywane w miejscu niedostępnym dla innych osób.
12. W uzasadnionych wyższą koniecznością i bezpieczeństwem badań przypadkach, po uprzednim wyrażeniu zgody przez Dyrektora, dopuszczalne jest czasowe wydanie klucza zapasowego, którego zwrot następuje niezwłocznie po usunięciu wyższej konieczności.

**Bezpieczne korzystanie z pomieszczeń**

1. Przed otworzeniem drzwi wejściowych i drzwi do poszczególnych pomieszczeń służbowych należy sprawdzić stan zamków oraz innych zastosowanych zabezpieczeń.

Po otworzeniu pomieszczeń należy zweryfikować stan zastosowanych zabezpieczeń pomieszczenia (np. okna), sprzętu i dokumentacji (np. szafy, plomby).

1. W trakcie korzystania z pomieszczenia Pracownicy odpowiadają za bezpieczeństwo przetwarzanych Danych osobowych. Osoby nieupoważnione do przetwarzania (np. ekipa remontowa) mogą przebywać w obszarze przetwarzania wyłącznie wówczas, kiedy przebywa w nim uprawniony Pracownik. Dane osobowe powinny być przetwarzane bez możliwości dostępu do wglądu dla osób nieupoważnionych. Jeśli takie zabezpieczenie nie jest możliwe należy wstrzymać się od przetwarzania w czasie obecności osób nieupoważnionych i zabezpieczyć poufność Danych osobowych.
2. Dane osobowe przetwarzane mogą być wyłącznie na stanowisku pracy. Zabronione jest pozostawianie dokumentów i nośników danych poza zabezpieczonymi pomieszczeniami, tj. korytarze, drukarki, kserokopiarki, pomieszczenia ogólnodostępne, wynoszenie na zewnątrz do miejsc publicznych.
3. W trakcie pracy z Danymi osobowymi Użytkownik zobowiązany jest zachować je w porządku i poufności, uniemożliwiając wgląd osobom nieupoważnionym (tzw. polityka czystego biurka, ekranu i kosza).
4. Dokumenty i nośniki, które zawierają Dane osobowe, w tym nieformalne notatki czy wydruki, należy niszczyć za pomocą niszczarki lub innej metody uniemożliwiającej identyfikację osób, których dane dotyczą.
5. Po zakończeniu pracy z Danymi osobowymi Użytkownicy zobowiązani są do uporządkowania swojego stanowiska pracy poprzez wykonanie czynności zabezpieczających Dane osobowe adekwatnych do zastosowanych rozwiązań technicznych i organizacyjnych, w szczególności:
6. zabezpieczenia poufności dokumentacji papierowej i elektronicznej a także elektronicznych nośników danych (np.przez ich zamknięcie w sejfie, biurkach, szafach do tego przeznaczonych i schowanie klucza w miejscu niedostępnym dla innych osób);
7. wyłączenia i zabezpieczenia urządzeń elektronicznych (projektorów, komputerów, drukarek, ekranów) i urządzeń zasilanych energią elektryczną (czajniki, grzejniki, wentylatory) zgodnie z zasadami BHP;
8. zabezpieczenia pieczątek i wszelkich poufnych zasobów;
9. zamknięcia okien i drzwi.

**Postępowanie w przypadku naruszenia**

1. W przypadku podejrzenia lub stwierdzenia jakichkolwiek naruszeń, w tym naruszeń zabezpieczeń fizycznych (drzwi, okna, zamki, szafy) należy niezwłocznie powiadomić Dyrektora lub osobę przez niego wskazaną i Inspektora, zgodnie z §11 Polityki.
2. W przypadku utraty, uszkodzenia lub zniszczenia kluczy bądź karty dostępu, Pracownik niezwłocznie powiadamia o tym fakcie bezpośredniego przełożonego i Inspektora.
3. Dorabianie kluczy do pomieszczeń Instytutu wymaga pisemnej zgody Dyrektora i dozwolone jest wyłącznie w celu zastąpienia kluczy uszkodzonych lub zniszczonych.
4. W przypadku zagubienia klucza konieczna jest wymiana całego zamka. W przypadku zagubienia karty dostępu osoba wskazana przez Dyrektora niezwłocznie dezaktywuje zagubioną kartę w systemie. W przypadku ryzyka ujawnienia kodu do systemu alarmowego kod zostaje usunięty z systemu i wymieniony na nowy.
5. Kody do systemu alarmowego winny być zmieniane nie rzadziej niż raz do roku.

*Załącznik nr 7 do Polityki Ochrony Danych osobowych w IBM PAN*

**Regulamin korzystania z Systemu informatycznego i zasobów elektronicznych w Instytucie**

1. Regulamin określa zasady korzystania z zasobów elektronicznych dostępnych dla Pracowników w Systemie informatycznym Instytutu. Zasobami elektronicznymi Instytutu są wszelkie dane należące do Instytutu, a zachowane w formie elektronicznej, niezależnie od nośnika na którym się znajdują.
2. System informatyczny przeznaczony jest do wspomagania działalności statutowej Instytutu, wymiany informacji pomiędzy ośrodkami naukowymi i badawczymi na całym świecie oraz do wspomagania zarządzania Instytutem, w tym przepływu komunikacji służbowej i wyłącznie do podejmowania aktywności związanej z tymi celami może być używany.
3. Każdy Pracownik odpowiada za powierzony mu sprzęt i oprogramowanie oraz korzystanie z Systemu informatycznego i Danych osobowych z dołożeniem należytej staranności oraz zgodnie z prawem. Zabronione jest udostępnianie przez Pracowników sprzętu, jak i oprogramowania osobom trzecim, tak odpłatnie, jak i nieodpłatnie.

**Konta pocztowe**

1. Konto pocztowe w domenie Instytutu powinien posiadać każdy Pracownik administracyjny oraz naukowy.
2. Konto pocztowe oraz dostęp do zasobów elektronicznych Instytutu udzielane są przy zatrudnieniu przez osobę odpowiedzialną za wsparcie informatyczne Instytutu na wniosek Działu Kadr w porozumieniu z bezpośrednim przełożonym.
3. Zablokowanie lub usunięcie konta pocztowego oraz blokada dostępu do zasobów elektronicznych Instytutu następuje na wniosek Działu Kadr w porozumieniu z bezpośrednim przełożonym, z dniem zakończenia współpracy lub z innej uzasadnionej przyczyny.
4. Informacja o adresie konta pocztowego utworzonego dla Pracownika jest jawna i może być powszechnie dostępna, w tym w witrynie internetowej Instytutu.
5. Pracownicy zobowiązani są do regularnego sprawdzania konta pocztowego oraz posługiwania się nim do realizacji elektronicznej korespondencji związanej z zadaniami realizowanymi dla Instytutu lub we współpracy z Instytutem.
6. Dostęp do konta pocztowego podlega odpowiednim zabezpieczeniom.
7. Hasło do konta pocztowego powinno być niepowtarzalne, zindywidualizowane, wybrane zgodnie ze standardami bezpieczeństwa (nie mniej niż 16 znaków, zawierać cyfry, duże i małe litery oraz znaki specjalne) i zachowane w poufności.
8. Wskazana jest regularna zmiana hasła przez Pracownika, nie rzadziej niż raz na kwartał.
9. Urządzenie służące do obsługi konta pocztowego musi być zabezpieczone aktualnym programem antywirusowym, a dostęp do niego powinien być zabezpieczony hasłem.
10. Zabronione jest otwieranie załączników i hiperłączy z nieznanych lub podejrzanych źródeł.
11. Przy prowadzeniu korespondencji elektronicznej Pracownik zobowiązany jest weryfikować listę odbiorców i poufność ich adresów (np. używać funkcji kopii ukrytej), wysyłać korespondencję tylko do osób, których ona dotyczy oraz każdorazowo szyfrować dokumenty zawierające dane osobowe. Hasło do dokumentów winno być przekazywane innym kanałem komunikacji (np. sms) lub znane obu stronom bez bezpośredniego ujawniania (np. PESEL).
12. Osoba odpowiedzialna za wsparcie informatyczne Instytutu prowadzi we współpracy z Działem Kadr ewidencję i cykliczną aktualizację założonych kont pocztowych zgodnie ze stanem zatrudnienia oraz użytecznością.

**Zasady korzystania z Systemu informatycznego**

1. Osobę odpowiedzialna za wsparcie informatyczne Instytutu we współpracy z Działem Kadr i bezpośrednim przełożonym sprawuje nadzór nad udzielaniem dostępu do Systemu informatycznego i jego zakresem, wdrażanym oprogramowaniem i licencjami, instalacją, konserwacją i inwentaryzacją posiadanego sprzętu komputerowego wraz z urządzeniami peryferyjnymi.
2. Każdy Pracownik posiada swój własny identyfikator (login) umożliwiający dostęp do Systemu informatycznego i zobowiązany jest korzystać z Systemu wyłącznie z jego użyciem.
3. Instytut zobowiązuje się dołożyć wszelkich starań w celu zapewnienia poprawnego działania Systemu informatycznego oraz zobowiązuje się do udzielenia wszelkiej możliwej pomocy w zagadnieniach związanych z jego obsługą.
4. Pracownik zobowiązany jest korzystać z Systemu informatycznego, w tym zabezpieczyć dostęp do komputera i jego zasobów, w sposób uniemożliwiający dostęp do niego osobom nieuprawnionym.
5. Wniosek o zakup nowego sprzętu lub oprogramowania podlega akceptacji Dyrektora i procedurom wskazanym w ustawie prawo zamówień publicznych.
6. Pracownik jest odpowiedzialny za odpowiednie zabezpieczenie danych znajdujących się w Systemie informatycznym. Zabezpieczenie danych może polegać w szczególności na:
7. korzystaniu z bezpiecznych haseł logowania i szyfrowaniu plików;
8. regularnym skanowaniu antywirusowym komputera;
9. archiwizacji danych i tworzeniu kopii zapasowych na zaszyfrowanych i bezpiecznych dyskach zewnętrznych;
10. blokowaniu dostępu do ekranu i zasobów Systemu w przypadku czasowego opuszczenia stanowiska pracy oraz wylogowaniu z Systemu i wyłączania stacji roboczej po zakończeniu pracy.
11. Na wniosek Pracownika bezpośredni przełożony lub Dyrektor Instytutu może zezwolić na użytkowanie Systemu informatycznego poza siedzibą Instytutu, pod warunkiem przestrzegania zasad bezpieczeństwa i poufności, w szczególności:
12. dane, zwłaszcza Dane osobowe, powinny być przetwarzane bez wglądu osób trzecich, w tym rodziny oraz zabezpieczone bezpiecznym hasłem;
13. dostęp do pulpitu komputera musi być zabezpieczony hasłem;
14. Pracownik korzysta wyłącznie z własnego połączenia do sieci Internet - zabronione jest korzystanie z sieci publicznych (np. supermarket, kawiarnia, lotnisko);
15. Sprzęt i dokumenty będą pod stałym nadzorem Pracownika przechowywane w sposób bezpieczny, tj niepozostawiane bez nadzoru, w szczególności w środkach transportu.
16. W przypadku używania zewnętrznych nośników danych Pracownik zobowiązany jest wcześniej wykonać skanowanie programem antywirusowym wszystkich danych zawartych na nośniku.
17. Za utworzenie kopii zapasowych danych w formie elektronicznej odpowiedzialny jest Pracownik pracujący na tych danych. Kopie zapasowe powinny być wykonywane regularnie, nie rzadziej niż raz na kwartał. Za utworzenie kopii zapasowych danych przechowywanych na serwerach odpowiada osobę odpowiadającą za wsparcie informatyczne Instytutu.

**Zasady korzystania z oprogramowania**

1. Pracownicy zobowiązani są do korzystania wyłącznie z oprogramowania i zasobów elektronicznych nabytych przez Instytut. Korzystanie z oprogramowania i zasobów elektronicznych odbywa się z poszanowaniem dla praw własności intelektualnej twórców i zasadami udzielonych licencji.
2. Osoba odpowiedzialna za wsparcie informatyczne Instytutu jest wyłącznie uprawniona do instalacji lub autoryzacji instalacji oprogramowania zakupionego przez Instytut na sprzęcie komputerowym należącym do Instytutu. Osoba wskazana przez Dyrektora prowadzi ewidencję oprogramowania i licencji dostępnych w Instytucie oraz odpowiada za bezpieczne przechowanie ich fizycznych nośników lub kodów aktywacyjnych.
3. Pracownik jest uprawniony do inicjacji instalacji aktualizacji oprogramowania już zainstalowanego na sprzęcie komputerowym należącym do Instytutu. W przypadku aparatury naukowej, która wyposażona jest w sprzęt komputerowy aktualizacja oprogramowania może odbywać się wyłącznie po uprzednim poinformowaniu osoby odpowiedzialnej za wsparcie informatyczne Instytutu o konieczności wykonania aktualizacji i weryfikacji przez nią źródła pochodzenia aktualizacji. Preferowanym sposobem pierwszej instalacji takiego oprogramowania jest za pośrednictwem firmy, od której zakupiono aparaturę.
4. Instalowanie i uruchamianie oprogramowania na licencji otwartej (tzw. open sorce) nie zakupionego przez Instytut dopuszczalne jest wyłącznie po uprzedniej weryfikacji licencji z radcą prawnym Instytutu. Zabrania się pobierania i kopiowania z Internetu wszelkich plików (programów komputerowych, utworów muzycznych, filmów, gier komputerowych, itp.) na sprzęt należący do Instytutu, a będących przedmiotem ochrony praw autorskich w przypadku braku posiadania stosownych uprawnień do ich wykorzystania w celach naukowo-badawczych, ze szczególnym uwzględnieniem możliwości komercjalizacji.

**Zasady bezpieczeństwa**

1. Zabronione jest ujawnianie jakichkolwiek zabezpieczeń zasobów elektronicznych, w tym haseł, osobom trzecim, w tym innym pracownikom Instytutu.
2. Stacje robocze służące do przetwarzania szczególnie istotnych Danych osobowych (tj. dane kadrowe, dane podpisu elektronicznego) powinny być przypisane do indywidualnego Użytkownika.
3. Zobowiązuje się Użytkowników do uważnego czytania i nieignorowania komunikatów i ostrzeżeń pojawiających się w przeglądarce dotyczących „alertów bezpieczeństwa”.
4. W przypadku wystąpienia zagrażającego bezpieczeństwu Danych osobowych należy niezwłocznie zgłosić takie zdarzenie do osoby odpowiedzialnej za wsparcie informatyczne Instytutu oraz Inspektora.
5. Poza przypadkami wskazanymi przez Dyrektora, pracownikom zabrania się działanie na szkodę bezpieczeństwa i integralności Systemu informatycznego Instytutu, w szczególności ingerencji fizycznej i systemowej w System informatyczny, w tym otwieranie lub usuwanie oznaczeń ze sprzętu komputerowego i urządzeń peryferyjnych, naruszanie bezpieczeństwa serwerów, instalację i uruchamianie niebezpiecznego lub nielegalnego oprogramowania.