DOKUMENTACJA PRZETWARZANIA DANYCH OSOBOWYCH

w CERES Management Services sp. z o.o.

Polityka bezpieczeństwa przetwarzania danych osobowych

Noerr Biedecki sp.k.
ul. Grzybowska 87
00-844 Warszawa
Polska

T +48 22 3788500
F +48 22 3788518
www.noerr.com

Alicante
Berlin
Bratislava
Brussels
Bucharest
Budapest
Dresden
Düsseldorf
Frankfurt/M.
Hamburg
London
Moscow
Munich
New York
Prague
Warsaw

KRS 0000178462,
Regon 015610089,
NIP 526-27-40-717

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

w CERES Management Services sp. z o.o.

1. Postanowienia ogólne

1.1. Niniejsza polityka bezpieczeństwa przetwarzania danych osobowych, zwana dalej „**Polityką bezpieczeństwa**" określa zasady bezpieczeństwa przetwarzania danych osobowych w CERES Management Services sp. z o.o. z siedzibą w Warszawie, zwanej dalej „**CERES**" i stanowi element Dokumentacji Przetwarzania Danych Osobowych w CERES.

1.2. Określone w niniejszej Polityce bezpieczeństwa zasady powinny być przestrzegane przez wszystkich pracowników i współpracowników CERES przetwarzających dane osobowe oraz mających dostęp do danych osobowych, w tym również praktykantów, stażystów, osoby współpracujące na podstawie umowy zlecenia lub umowy o dzieło.

1.3. Określone w niniejszej Polityce bezpieczeństwa zasady dotyczą również przetwarzania danych osobowych powierzonych CERES do przetwarzania na podstawie odrębnej umowy, w stosunku do których CERES występuje w charakterze podmiotu przetwarzającego (procesora) w rozumieniu art. 28 RODO.

1.4. Zasady przetwarzania danych osobowych określone w niniejszej Polityce bezpieczeństwa służą zapewnieniu rzetelnej ochrony danych osobowych przetwarzanych przez CERES zgodnie z postanowieniami rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 85/46/WE (zwanym dalej „**RODO**") oraz przepisami krajowymi uchwalonymi w wykonaniu lub w związku z RODO, zwanymi dalej łącznie „**Przepisami**", w tym zabezpieczeniu danych przed dostępem do nich osób nieuprawnionych, przed zmianą lub zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Przepisów oraz utratą, uszkodzeniem lub zniszczeniem.

1.5. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w CERES rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych ustalanego w oparciu o przeprowadzoną ocenę skutków przetwarzania danych.

1.6. Zastosowane zabezpieczenia mają służyć osiągnięciu celów określonych w pkt 1.4 powyżej i zapewnić:

a. poufność danych – oznaczającą, że dane osobowe nie są udostępniane podmiotom nieuprawnionym i nieupoważnionym,

b. integralność danych – oznaczającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

c. rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby lub podmiotu mogą być przypisane w sposób jednoznaczny tylko tej osobie lub temu podmiotowi,

d. integralność systemu – oznaczającą niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej,

e. uzasadnioną dostępność informacji – oznaczająca, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wyłącznie wówczas, gdy jest to potrzebne i w zakresie, w jakim jest to niezbędne,

f. efektywne zarządzanie ryzykiem – rozumiane jako kontrolowanie i minimalizowanie lub eliminowanie ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

1.7. Politykę bezpieczeństwa stosuje się do danych osobowych przetwarzanych w formie papierowej, w systemach informatycznych, danych osobowych zapisanych na zewnętrznych nośnikach informacji oraz informacji dotyczących bezpieczeństwa przetwarzania danych osobowych, w szczególności dotyczących wdrożonych w CERES zabezpieczeń technicznych i organizacyjnych.

1.8. Każdy pracownik oraz osoba współpracująca z CERES na podstawie innej niż umowa o pracę przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej odbywa szkolenie w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych. Zakres szkolenia obejmuje w szczególności zaznajomienie z Przepisami oraz wydanymi na ich podstawie aktami wykonawczymi oraz procedurami i instrukcjami obowiązującymi w CERES w zakresie ochrony danych osobowych.

1.9. Szkolenie zostaje zakończone podpisaniem przez osobę oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych. Dokument ten jest przechowywany w aktach osobowych pracownika lub w dokumentacji dotyczącej osoby współpracującej niebędącej pracownikiem i stanowi podstawę do podejmowania działań w celu nadania im uprawnień do korzystania z systemu informatycznego przetwarzającego dane osobowe. Wzór oświadczenia stanowi Załącznik nr 4 do niniejszej Polityki bezpieczeństwa.

1.10. Pojęcia niezdefiniowane w niniejszej Polityce bezpieczeństwa mają znaczenie nadane im w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, Procedurze zgłaszania naruszeń ochrony danych osobowych i innych procedurach i dokumentach tworzących Dokumentację Przetwarzania Danych Osobowych w CERES.

2. Przetwarzanie danych osobowych

2.1. Administratorem danych osobowych jest CERES Management Services sp. z o.o. z siedzibą w Warszawie (00-803) Al. Jerozolimskie 56C, wpisana do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego pod numerem KRS 0000576925, zwana dalej „**Administratorem**".

2.2. Dane osobowe powinny być chronione przez każdą osobę przetwarzającą je przed nieuprawnionym dostępem i modyfikacją.

2.3. Przetwarzanie danych osobowych jest dozwolone wyłącznie przez osoby uprawnione w świetle Przepisów lub posiadające upoważnienie wydane przez Administratora. Wzór upoważnienia stanowi Załącznik nr 1 do niniejszej Polityki bezpieczeństwa.

2.4. Upoważnienie do przetwarzania danych osobowych wydawane jest przez Administratora indywidualnie przed rozpoczęciem przetwarzania danych osobowych. Upoważnienie do przetwarzaniach danych osobowych jest wydawane w trzech egzemplarzach: jeden dla osoby upoważnionej i dwa dla Administratora.

2.5. Administrator przechowuje upoważnienie do przetwarzania danych osobowych w dokumentacji ochrony danych osobowych, a jeden egzemplarz w aktach osobowych pracownika lub w dokumentacji dotyczącej osoby współpracującej niebędącej pracownikiem.

2.6. Modyfikacji lub odwołania upoważnienia dokonuje Administrator.

2.7. Ewidencja osób upoważnionych do przetwarzania danych osobowych jest prowadzona przez Administratora, zgodnie ze wzorem stanowiącym Załącznik nr 2 do niniejszej Polityki i zawiera w szczególności:

a. imię i nazwisko osoby upoważnionej do przetwarzania danych osobowych,

b. zakres upoważnienia do przetwarzania danych osobowych,

c. datę nadania uprawnień,

d. datę ustania uprawnień.

2.8. Do obowiązków osób upoważnionych do przetwarzania danych osobowych należy:

a. przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa oraz przyjętymi regulacjami, w tym zgodnie z Polityką bezpieczeństwa i Przepisami,

b. zachowania w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia, również po ustaniu zatrudnienia lub współpracy z CERES,

c. postępowania zgodnie z ustalonymi regulacjami dotyczącymi przetwarzania danych osobowych obowiązującymi w CERES,

d. ochrony danych osobowych przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem,

e. nieujawnianie Haseł dostępu do komputera i innych nośników danych, na których przetwarzane są dane osobowe, jak również do Systemów informatycznych, za pomocą których przetwarzane są dane osobowe,

f. zabezpieczenie stanowiska pracy po zakończeniu pracy, w szczególności zabezpieczenie wszelkiej dokumentacji, wydruków, elektronicznych nośników informacji i umieszczenie ich w zamykanych szafkach,

g. ustawienie monitora w taki sposób, aby uniemożliwić podgląd wyświetlanych danych osobowych przez osoby nieuprawnione (np. tyłem do okna, drzwi, itp.),

h. nieinstalowanie oprogramowania na komputerze ani na innym elektronicznym nośniku danych bez wcześniejszej pisemnej zgody Administratora lub upoważnionej przez niego osoby zarządzającej systemami IT,

i. niezwłocznego informowania przełożonego lub bezpośrednio Administratora o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe.

2.9. Każda osoba mająca styczność z danymi osobowymi jest zobowiązana do ochrony danych osobowych oraz przetwarzania ich wyłącznie w granicach udzielonego jej upoważnienia.

2.10. Naruszenie przez osobę upoważnioną do przetwarzania danych osobowych zasad bezpieczeństwa przetwarzania danych prowadzić będzie do wszczęcia przez Administratora właściwego postępowania wobec takiej osoby. Naruszenie zasad bezpieczeństwa przetwarzania danych, w zależności od okoliczności zdarzenia, może zostać zakwalifikowane jako:

a. ciężkie naruszenie podstawowych obowiązków pracowniczych i uzasadniać natychmiastowe rozwiązanie umowy o pracę bez wypowiedzenia,

b. naruszenie istotnych postanowień umowy cywilnoprawnej i uzasadniać natychmiastowe jej rozwiązanie.

2.11. Upoważnienie do przetwarzania danych osobowych jest odwoływane niezwłocznie w razie:

a. rozwiązania umowy o pracę w związku z zawartym porozumieniem, w wyniku upływu okresu wypowiedzenia lub rozwiązania umowy o pracę bez zachowania okresu wypowiedzenia,

b. wygaśnięcia stosunku pracy,

c. rozwiązania lub wygaśnięcia umowy cywilnoprawnej zawartej z osobą upoważnioną do przetwarzania danych osobowych,

d. tymczasowego aresztowania lub pozbawienia wolności osoby upoważnionej do przetwarzania danych osobowych,

e. niestawienia się osoby upoważnionej do przetwarzania danych osobowych bez usprawiedliwienia do pracy.

2.12. Odwołanie upoważnienia skutkuje natychmiastowym zablokowaniem konta Użytkownika Systemu informatycznego i Identyfikatora nadanych osobie upoważnionej do przetwarzania danych osobowych, zgodnie z postanowieniami Instrukcji zarządzania systemem informatycznym obowiązującej w CERES.

2.13. Administrator może zawiesić uprawnienia osoby upoważnionej do przetwarzania danych osobowych, w szczególności w razie długotrwałej nieobecności spowodowanej niezdolnością do pracy wskutek choroby, urlopem macierzyńskim, rodzicielskim, bezpłatnym, w razie wszczęcia postępowania wyjaśniającego lub dyscyplinarnego.

2.14. Dane osobowe można przetwarzać wyłącznie za pomocą urządzeń służbowych i oprogramowania wykorzystywanego w CERES w celach służbowych. Niedozwolone jest kopiowanie ani powielanie danych osobowych w jakiejkolwiek postaci, w jakikolwiek sposób i na jakimkolwiek nośniku, jeżeli stworzenie kopii lub powielanie nie jest niezbędne do przetwarzania danych zgodnie z niniejszą Polityką bezpieczeństwa lub Przepisami.

2.15. Administrator może powierzyć inspektorowi ochrony danych, jeśli zostanie powołany w CERES, udzielanie, modyfikowanie, zawieszanie i/lub odwoływanie upoważnień,

prowadzenie ewidencji osób upoważnionych oraz przechowywanie dokumentacji w tym zakresie.

3. Zbiory danych osobowych

3.1. Wzór wykazu zbiorów danych osobowych wraz ze wskazaniem zakresu przetwarzanych danych osobowych stanowi Załącznik nr 3 do niniejszej Polityki bezpieczeństwa.

3.2. CERES nie tworzy zbiorów danych osobowych ani nie przetwarza danych w zakresie innym, aniżeli wynikający z niniejszej Polityki bezpieczeństwa oraz wykazu zbiorów danych osobowych.

3.3. W razie ujawnienia lub dostarczenia przez osobę fizyczną do CERES danych osobowych w zakresie wykraczającym poza wskazany w pkt 3.1 powyżej, osoba, której takie dane przekazano zobowiązana jest je natychmiast usunąć (zniszczyć, zaczernić, zamazać) lub w inny sposób trwale zapobiec ich dalszemu przetwarzaniu.

3.4. CERES nie przetwarza danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, jak również danych genetycznych, biometrycznych, dotyczących zdrowia, seksualności lub orientacji seksualnej osoby, chyba, że przetwarzanie takich danych jest dopuszczalne an podstawie obowiązujących przepisów prawa.

4. Obszar przetwarzania danych, określenie środków technicznych i organizacyjnych

4.1. Dane osobowe mogą być przetwarzane wyłącznie w obszarach przetwarzania danych osobowych, na które składają się pomieszczenia biurowe oraz części pomieszczeń, gdzie CERES prowadzi działalność, w szczególności:

a. pomieszczenia biurowe, w których zlokalizowane są komputery służące do przetwarzania danych osobowych,

b. pomieszczenia, w których przechowuje się dokumenty źródłowe oraz wydruki z systemu informatycznego zawierające dane osobowe,

c. pomieszczenia, w których przechowywane są urządzenia, elektroniczne nośniki informacji oraz kopie zapasowe zawierające dane osobowe.

4.2. Wzór wykazu budynków i pomieszczeń, w których przetwarzane są dane osobowe stanowi Załącznik nr 5 do niniejszej Polityki bezpieczeństwa.

4.3. Pomieszczenia wchodzące w skład obszaru przetwarzania danych osobowych są wyposażone w odpowiednie środki ochrony fizycznej i organizacyjnej chroniące przed

nieautoryzowanym lub nieuprawnionym dostępem, uszkodzeniem lub zakłóceniem pracy.

4.4. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane podczas nieobecności osób upoważnionych do przetwarzania danych osobowych, w sposób ograniczający możliwość dostępu do nich osobom nieupoważnionym.

4.5. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe w czasie ich chwilowej nieobecności w takim pomieszczeniu w trakcie pracy, jak również po zakończeniu pracy. Klucze do pomieszczeń nie mogą być pozostawione w zamku drzwi i powinny być przechowywane wyłącznie w miejscu przeznaczonym do ich przechowywania.

4.6. Dokumentacja papierowa po godzinach pracy CERES jest przechowywana w zamykanych biurkach lub szafach.

4.7. Urządzenia służące do przetwarzania danych osobowych należy przechowywać w bezpieczny i nadzorowany sposób.

4.8. Dostęp do pomieszczeń wchodzących w skład obszaru przetwarzania danych osobowych jest monitorowany.

4.9. Dla zapewnienia ciągłości działania systemów informatycznych służących do przetwarzania danych osobowych stosuje się w nich sprzęt oraz oprogramowanie wyprodukowane przez renomowanych producentów oraz zabezpiecza się sprzęt przed awarią zasilania i zakłóceniami w sieci zasilającej.

4.10. Zbiory danych osobowych oraz programy służące do przetwarzania danych osobowych są zabezpieczane przed przypadkową utratą albo celowym zniszczeniem poprzez wykonywanie kopii zapasowych. Procedura tworzenia kopii zapasowych została opisana w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

4.11. Urządzenia mobilne, w tym komputery przenośne, tablety, telefony komórkowe, itp., nie powinny być pozostawiane przez ich posiadacza bez opieki, jeżeli nie są zastosowane odpowiednie środki ochrony.

4.12. Wydruki i nośniki elektroniczne zawierające dane osobowe należy przechowywać w zamykanych szafach, które znajdują się w obszarach przetwarzania danych osobowych.

4.13. Przebywanie osób nieuprawnionych w obszarze przetwarzania danych osobowych jest dopuszczalne wyłącznie w obecności osoby upoważnionej do przetwarzania danych osobowych lub za zgodą wyznaczonej osoby.

5. Udostępnianie danych osobowych

5.1. Udostępnianie danych osobowych może nastąpić wyłącznie za zgodą Administratora.

5.2. Dane osobowe mogą być udostępniane wyłącznie podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa oraz osobom, których dotyczą.

5.3. Informacje zawierające dane osobowe powinny być przekazywane uprawnionym podmiotom lub osobom, których dotyczą listem poleconym za potwierdzeniem odbioru lub innym bezpiecznym sposobem, wynikającym z przepisów prawa lub umowy.

5.4. Udostępniając dane osobowe należy odnotowywać informacje o udostępnieniu, w tym informację o odbiorcy danych, dacie oraz zakresie udostępnionych danych osobowych. Wzór rejestru udostępnień danych osobowych stanowi załącznik nr 6 do niniejszej Polityki bezpieczeństwa.

5.5. Udostępniając dane osobowe należy zaznaczyć, że podmiot, któremu je udostępniono może je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

6. Powierzenie przetwarzania danych osobowych

6.1. Przetwarzanie danych osobowych, których administratorem jest CERES, dokonywane w imieniu CERES przez podmiot trzeci, może mieć miejsce wyłącznie po uprzednim zawarciu umowy powierzenia przetwarzania danych.

6.2. Umowa powierzenia przetwarzania danych może być zawarta wyłącznie z podmiotem zapewniającym gwarancję wdrożenia odpowiednich środków technicznych i organizacyjnych zapewniających, aby spełniały one postanowienia RODO oraz gwarantowały ochronę praw osób, których te dane dotyczą.

6.3. Umowa powierzenia przetwarzania danych powinna zawierać w szczególności zapisy dotyczące: danych podmiotu przetwarzającego, przedmiotu, charakteru, celu i czasu trwania powierzenia przetwarzania, kategorii osób, których przetwarzane dane dotyczą oraz obowiązków i praw CERES.

6.4. CERES jest uprawniony do dokonywania u podmiotów, którym powierzył przetwarzanie danych osobowych audytów i inspekcji w celu zbadania zgodności przetwarzania danych z Przepisami i umową powierzenia przetwarzania danych.

6.5. Podpowierzanie przetwarzania danych nie jest dopuszczalne, o ile CERES i podmiot, któremu powierzono przetwarzanie danych nie postanowią inaczej na piśmie.

6.6. Powierzenie przetwarzania danych osobowych, których procesorem jest CERES i które przetwarzane są przez CERES na rzecz podmiotu trzeciego, może mieć miejsce wyłącznie wówczas, gdy zostanie to uprzednio uzgodnione z administratorem tych danych lub jest dopuszczalne w świetle umowy powierzenia przetwarzania danych łączącej CERES z takim administratorem.

7. Usuwanie danych

7.1. Wydruki lub inne dokumenty zawierające dane osobowe, które nie będą już wykorzystywane przy przetwarzaniu tych danych należy niezwłocznie zniszczyć w sposób zgodny z procedurą usuwania danych.

7.2. CERES sprawuje kontrolę i nadzór nad procesem usuwania i niszczenia danych osobowych zbędnych oraz takich, o których usunięcie zawnioskowała osoba, której dane dotyczą.

7.3. Usuwanie i niszczenie danych osobowych polega na:

a. fizycznym trwałym zniszczeniu danych i/lub ich nośników w sposób uniemożliwiający ich odtworzenie lub

b. pozbawienie danych cech pozwalających na późniejszą identyfikację osób fizycznych, których te dane dotyczą (tzw. anonimizacja danych).

7.4. Zniszczenie danych i/lub ich nośnika jest dokumentowane protokołem zniszczenia. Protokół zniszczenia jest przechowywany przez CERES lub inspektora ochrony danych, jeśli zostanie powołany w CERES.

7.5. Usunięcie danych osobowych może nastąpić również na wniosek osoby, której dane dotyczą i w zakresie złożonego wniosku, o ile dalsze przetwarzanie takich danych nie jest wymagane powszechnie obowiązującymi przepisami prawa lub umową obowiązującą pomiędzy CERES i osobą, której dane dotyczą.

7.6. Wniosek o usunięcie danych wraz z adnotacją o ich usunięciu jest przechowywany przez CERES lub inspektora ochrony danych, jeśli zostanie powołany w CERES.

8. Inspektor ochrony danych

8.1. Administrator może powołać inspektora ochrony danych.

8.2. Inspektorem ochrony danych może być osoba posiadająca wiedzę w obszarze ochrony danych osobowych, znająca organizację CERES oraz technologie i stosowane przez CERES rozwiązania informatyczne w zakresie umożliwiającym zapewnienie zgodności procesów przetwarzania danych osobowych w CERES z Przepisami.

8.3. Inspektor ochrony danych może wyznaczyć swojego zastępcę. Zastępca inspektora ochrony danych powinien posiadać cechy wskazane w pkt 9.2 powyżej. W przypadku nieobecności inspektora ochrony danych przekraczającej 2 tygodnie wskazanie zastępcy na czas takiej nieobecności jest obowiązkowe.

9. Postanowienia końcowe

9.1. Każdy pracownik CERES oraz każda osoba współpracująca z CERES na podstawie umowy cywilnoprawnej jest zapoznawana z Przepisami i zobowiązuje się do ich przestrzegania.

9.2. W sprawach nieuregulowanych w niniejszej Polityce bezpieczeństwa mają zastosowanie Przepisy.

10. Załączniki:

10.1. Załącznik nr 1 – Wzór upoważnienia do przetwarzania danych osobowych.

10.2. Załącznik nr 2 – Wzór rejestru osób upoważnionych do przetwarzania danych.

10.3. Załącznik nr 3 – Wzór wykazu zbiorów danych osobowych.

10.4. Załącznik nr 4 – Wzór oświadczenia o przestrzeganiu zasad i przepisów ochrony danych osobowych i o zachowaniu tajemnicy danych osobowych.

10.5. Załącznik nr 5 – Wzór wykazu obszarów przetwarzania danych osobowych.

10.6. Załącznik nr 6 – Wzór rejestru udostępnień danych osobowych.

10.7. Załącznik nr 7 – Szablon wykazu podmiotów zewnętrznych, którym powierzono dane do przetwarzania.

.....

(w imieniu Ceres Management Services Sp. Z o.o.)

Załącznik nr 1 do Polityki bezpieczeństwa przetwarzania danych osobowych

.....

(data nadania upoważnienia)

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym udzielam Panu/Pani*:

.....

(imię i nazwisko)

.....

(stanowisko służbowe)

upoważnienia do przetwarzania danych osobowych.

Jest Pan/Pani* upoważniony/upoważniona* do przetwarzania, w tym w systemie informatycznym, danych osobowych wyłącznie w zakresie wynikającym z Pana/Pani* zadań służbowych oraz poleceń przełożonego.

Upoważnienie traci ważność z chwilą jego odwołania oraz w każdym wypadku z chwilą *ustania stosunku pracy / zakończenia współpracy*.

.....

(data i podpis osoby upoważniającej)

Oświadczam, że zapoznała(e)m się, rozumiem i będę przestrzegać obowiązków wynikających z przepisów 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 85/46/WE, aktów prawa krajowego wydanych na jego podstawie lub w związku z nim oraz dokumentów związanych z przetwarzaniem danych osobowych w CERES Management Services sp. z o.o., w szczególności Polityki bezpieczeństwa przetwarzania danych osobowych.

Zobowiązuję się do zapewnienia bezpieczeństwa przetwarzania danych osobowych poprzez ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem.

Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których uzyskam dostęp w trakcie zatrudnienia/współpracy oraz po jego ustaniu.

Przyjmuję do wiadomości, że za niedopełnienie obowiązków wynikających z niniejszego oświadczenia ponoszę odpowiedzialność na podstawie przepisów prawa.

.....

(data i podpis pracownika)

Załącznik nr 2 do Polityki bezpieczeństwa przetwarzania danych osobowych

Wzór rejestru osób upoważnionych do przetwarzania danych osobowych w CERES Management Services sp. z o.o.

Lp.	Imię i nazwisko	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia		Login	Uwagi
				Stanowisko służbowe	Dostęp do oprogramowania (nazwy systemów i zbiorów, do których użytkownik ma dostęp)		
1.							
2.							
...							

Załącznik nr 3 do Polityki bezpieczeństwa przetwarzania danych osobowych

Wzór wykazu zbiorów danych osobowych w CERES Management Services sp. z o.o.

Lp.	Nazwa zbioru	Podstawa prawna przetwarzania danych	Cel przetwarzania danych	Zakres przetwarzanych danych	Program komputerowy zastosowany do przetwarzania danych w zbiorze	Kategorie odbiorców, którym dane mogą zostać ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych
1.						

Załącznik nr 4 do Polityki bezpieczeństwa przetwarzania danych osobowych

Wzór oświadczenia o przestrzeganiu zasad i przepisów ochrony danych osobowych i o zachowaniu tajemnicy danych osobowych

.....
(imię i nazwisko)

.....
(miejscowość, data)

Oświadczenie

Oświadczam, że zostałem/zostałam* zapoznany/zapoznana* z:

- przepisami o ochronie danych osobowych,
- zasadami przetwarzania i ochrony danych osobowych opisanymi w obowiązujących w CERES Management Services sp. z o.o. Polityce bezpieczeństwa przetwarzania danych osobowych, Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz innych przepisach i instrukcjach wewnętrznych wdrożonych do stosowania w CERES Management Services sp. z o.o.

Jednocześnie oświadczam, że zobowiązuję się przestrzegać zasad i przepisów z zakresu ochrony danych osobowych oraz informacji objętych prawem tajemnicy przedsiębiorstwa podczas wykonywania obowiązków służbowych, w tym zobowiązuję się do:

- dołożenia wszelkich starań przy wykonywaniu powierzonych mi obowiązków w celu ochrony danych osobowych i informacji prawem chronionych,
- przetwarzania danych osobowych zgodnie z obowiązującymi w tym zakresie przepisami prawa i regulacjami wewnętrznymi administratora danych,
- do zabezpieczenia przetwarzanych danych przed ich:
  a) udostępnieniem osobom nieupoważnionym,
  b) zabraniem przez osobę nieuprawnioną,
  c) przetwarzaniem z naruszeniem przepisów prawa,
  d) nieuprawnioną zmianą, zniszczeniem lub utratą,
- do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, również po ustaniu zatrudnienia.

.....
(podpis osoby składającej oświadczenie)

Załącznik nr 5 do Polityki bezpieczeństwa przetwarzania danych osobowych

Wzór wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w których przetwarzane są dane osobowe w CERES Management Services sp. z o.o.

1.	Wykaz pomieszczeń, w których przetwarzane są dane osobowe	
2.	Wykaz pomieszczeń, w których znajdują się komputery stanowiące element systemu informatycznego	
3.	Wykaz pomieszczeń, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające komputerowe nośniki informacji z kopiami zapasowymi danych, stacje komputerowe, serwery i inne urządzenia komputerowe)	
4.	Wykaz pomieszczeń, w których składowane są uszkodzone komputerowe nośniki danych (taśmy, dyski, płyty CD, dyski przenośne, uszkodzone komputery)	
5.	Wykaz pomieszczeń archiwum	
6.	Wykaz programów, w których przetwarzane są dane osobowe	
7.	Wykaz podmiotów zewnętrznych, które mają dostęp do danych osobowych lub je przetwarzają na podstawie podpisanych umów (np. informatyk) – nazwa firmy, imię, nazwisko, adres, funkcja.	
8.	Inne (proszę podać inne informacje dotyczące pomieszczeń, w których przetwarzane są dane osobowe oraz ich zabezpieczeń).	

Załącznik nr 6 do Polityki bezpieczeństwa przetwarzania danych osobowych

Wzór rejestru udostępnień danych osobowych w CERES Management Services sp. z o.o.

Lp.	Data	Dane osoby / podmiotu, któremu udostępniono dane	Forma / sposób udostępnienia danych	Zakres udostępnionych danych	Uwagi
1.					
2.					
...					

Załącznik nr 7 do Polityki bezpieczeństwa przetwarzania danych osobowych

Szablon wykazu podmiotów zewnętrznych, którym powierzono dane osobowe do przetwarzania przez CERES Management Services sp. z o.o.

Lp.	Nazwa podmiotu	Zakres świadczonych usług	Numer / data umowy	Uwagi (czy są zapisy w umowie związane z poufnością i odpowiedzialnością w stosunku do powierzonych danych, czy została zawarta odrębna umowa powierzenia przetwarzania danych)
1.				
2.				
...				