Załącznik
do Zarządzenia Nr 12/2015
Dyrektora Instytutu Spawalnictwa
Z dnia 01.12.2015 r.

POLITYKA BEZPIECZEŃSTWA W ZAKRESIE OCHRONY DANYCH OSOBOWYCH W INSTYTUCIE SPAWALNICTWA W GLIWICACH

Na podstawie art. 7 pkt. 4 i art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz.U. z 2014 r. poz. 1182 z późn. zm.) oraz § 3 i § 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz.1024) **ustalam następujące wytyczne polityki bezpieczeństwa w zakresie ochrony danych osobowych przetwarzanych w Instytucie Spawalnictwa w związku z realizacją zadań statutowych Instytutu.**

§ 1

Dyrekcja Instytutu świadoma wagi problemów związanych z ochroną prawa do prywatności, w tym w szczególności prawa osób fizycznych powierzających Instytutowi swoje dane osobowe do właściwej i skutecznej ochrony tych danych, deklaruje podejmowanie niezbędnych działań dla zapewnienia:

- bezpieczeństwa przetwarzania danych osobowych,
- stałego podnoszenia kwalifikacji osób przetwarzających dane osobowe w zakresie problematyki bezpieczeństwa przetwarzania tych danych,
- traktowania obowiązków osób zatrudnionych przy przetwarzaniu danych osobowych jako należących do kategorii podstawowych obowiązków pracowniczych oraz stanowczego egzekwowania ich wykonywania przez zatrudnione osoby,
- współpracy z instytucjami powołanymi do ochrony danych osobowych.

§ 2

1. „Polityka bezpieczeństwa w zakresie ochrony danych osobowych w Instytucie Spawalnictwa", zwana dalej „**Polityką**", jest dokumentem mającym na celu określenie podstawowych reguł dotyczących zapewnienia ochrony danych osobowych przetwarzanych w zbiorach danych:
   a) tradycyjnych, w szczególności w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych,
   b) w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych osobowych.
2. W Instytucie Spawalnictwa, zwanym dalej **Instytutem**, dane osobowe przetwarzane są z poszanowaniem obowiązujących w tym zakresie przepisów prawa, a w szczególności:
   a) przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz.U. z 2014 r. poz. 1182 z późn. zm.), zwanej dalej **Ustawą**, oraz przepisów wykonawczych z nią związanych,
   b) przepisów art.22^1 §1 - 5 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (tj. Dz.U. z 2014 r. poz. 1502 z późn. zm.) i przepisów wykonawczych z nią związanych,

c) innych przepisów ustaw i rozporządzeń normujących przetwarzanie danych osobowych określonych kategorii.

3. W Instytucie dane osobowe przetwarzane są w celu realizacji zadań statutowych. W szczególności dane osobowe przetwarza się:
   a) dla zapewnienia prawidłowego wykonania zadań statutowych Instytutu wynikających z przepisów ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych (tj. Dz. U. z 2015 r. poz. 1095) oraz określonych w Statucie Instytutu Spawalnictwa,
   b) w celu prowadzenia prawidłowej, zgodnej z prawem i zadaniami Instytutu, polityki personalnej oraz bieżącej obsługi stosunków zatrudnienia nawiązywanych przez Instytut działający jako pracodawca w rozumieniu art. 3 kodeksu pracy,
   c) dla realizacji innych usprawiedliwionych celów i zadań Instytutu – z poszanowaniem praw i wolności osób powierzających Instytutowi swoje dane.

§ 3

1. Instytut stosując reguły Polityki dokłada szczególnej staranności w celu ochrony interesów osób, których przetwarzane dane dotyczą, a w szczególności zapewnia, aby dane te były:
   a) przetwarzane zgodnie z prawem,
   b) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
   c) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
   d) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.
2. Pod szczególną ochroną pozostają wrażliwe dane osobowe wymienione w art. 27 ust.1 Ustawy. Przetwarzanie danych ujawniających: pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym, dopuszczalne jest tylko w związku z realizacją zadań statutowych Instytutu i w granicach wynikających z przepisów art. 27 ust. 2 Ustawy.

§ 4

Realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych, Instytut systematycznie dąży do unowocześniania stosowanych na jego terenie informatycznych, technicznych i organizacyjnych środków ochrony tych danych w celu ich zabezpieczenia przed udostępnieniem osobom nieupoważnionym, zawłaszczeniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy, zmianą, utratą, uszkodzeniem lub zniszczeniem.

§ 5

Instytut, realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych, prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki ochrony tych danych. W skład tej dokumentacji wchodzi Zarządzenie Dyrektora Instytutu

Spawalnictwa w sprawie ochrony danych osobowych w Instytucie Spawalnictwa, zawierające jako integralne części:

- niniejszą Politykę,
- „Instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Instytucie Spawalnictwa w Gliwicach",
- „Instrukcję postępowania w sytuacji naruszenia systemu ochrony danych osobowych w Instytucie Spawalnictwa w Gliwicach".

§ 6

Ilekroć w Polityce jest mowa o:

Zbiorze danych osobowych – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

Strukturze zbiorów danych – rozumie się przez to sposób składowania danych na komputerze polegający na grupowaniu logicznie powiązanych ze sobą danych różnego typu w jednym obszarze pamięci tak, by mogły być efektywnie wykorzystane. Składowe struktury - pola - są etykietowane, tj. mają swoje unikatowe nazwy; poprzez podanie nazwy otrzymuje się dostęp do danego pola.

Administratorze danych osobowych (ADO) - rozumie się przez to Dyrektora Instytutu

Administratorze bezpieczeństwa informacji (ABI) - rozumie się przez to osobę powołaną przez ADO, odpowiedzialną za bezpieczeństwo danych osobowych przetwarzanych w Instytucie.

Administratorze systemu informatycznego (ASI), zastępcy ASI - rozumie się przez to osoby powołane przez ADO do realizacji zadań technicznych związanych z bezpieczną eksploatacją urządzeń i aplikacji wykorzystywanych do przetwarzania danych osobowych w Instytucie.

Systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Bezpieczeństwie systemu informatycznego - rozumie się przez to środki organizacyjne i techniczne wdrożone przez ADO lub osobę przez niego upoważnioną, w celu ochrony danych przed dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem.

Przetwarzaniu danych osobowych - rozumie się przez to wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.

Osobie upoważnionej - rozumie się przez to osobę posiadającą upoważnienie wydane przez ABI i dopuszczoną w zakresie wskazanym w tym upoważnieniu do przetwarzania danych osobowych w systemie informatycznym i wersji papierowej. Ewidencję osób upoważnionych prowadzi ABI.

§ 7

1. Instytut, realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych, sprawuje nadzór nad rodzajami oraz zawartością zbiorów danych osobowych tworzonych na jego obszarze.
2. Wykaz baz danych, w których przetwarzane są dane osobowe w Instytucie zawiera załącznik nr 1 do niniejszej Polityki dostępny w wersji papierowej w Dziale Spraw Pracowniczych (IP).

§ 8

1. Realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych, Instytut udostępnia przetwarzane na jego obszarze dane osobowe wyłącznie osobom do tego upoważnionym na mocy uregulowań wewnętrznych.
2. Upoważnienie (wzór – załącznik nr 2), o którym mowa w ust. 1, wynikać może w szczególności:
   a) z charakteru pracy wykonywanej na danym stanowisku pracy,
   b) z zakresu obowiązków wykonywanych na danym stanowisku pracy, wynikających z karty osobowej,
   c) z odrębnego dokumentu zawierającego imienne upoważnienie do dostępu do danych osobowych.
3. Pracownicy posiadający upoważnienie do przetwarzania danych osobowych zobowiązani są aktualizować pod względem prawnym dokumenty na podstawie, których przetwarzają dane osobowe.
4. Pracownicy posiadający upoważnienie do przetwarzania danych zobowiązani są brać aktywny udział we wdrażaniu mechanizmów bezpieczeństwa poprzez opiniowanie możliwości zastosowania określonego rozwiązania przy realizacji ich obowiązków.
5. Pracownicy posiadający upoważnienie do przetwarzania danych zobowiązani są informować ABI o nowych elementach zbioru danych osobowych za który są odpowiedzialni celem aktualizacji rejestru zbiorów danych, który prowadzi ABI.

§ 9

Instytut, realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych, zapewnia dostęp do przetwarzanych danych osobowych osobom fizycznym będącym dysponentami tych danych.

§ 10

1. Osoby niezatrudnione przy przetwarzaniu danych osobowych określonej kategorii, w tym dysponenci danych osobowych, mające interes prawny lub faktyczny w uzyskaniu dostępu do tych danych, mogą mieć do nich wgląd wyłącznie w obecności upoważnionego pracownika Instytutu.
2. Udostępnianie danych osobowych pracowników Instytutu podmiotom zewnętrznym może odbywać się wyłącznie za pośrednictwem ABI lub ASI.
3. Udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
4. Zasada wyrażona w ust. 1 ma także zastosowanie do przypadku korzystania przez związki zawodowe z uprawnień przysługujących im na mocy Kodeksu pracy i ustawy z dnia 23 maja 1991 r. o związkach zawodowych (tj. Dz. U. z 2014 r. poz.167 z późn. zm.).

5. Udostępnienie danych osobowych bez pośrednictwa ABI lub ASI będzie uważane za naruszenie, o którym mowa w § 16.

§ 11

1. Zgodnie z art. 31 Ustawy, ADO może powierzyć, w drodze pisemnej umowy, przetwarzanie danych osobowych innemu podmiotowi.
2. O konieczności powierzenia danych do przetwarzania z zastosowaniem technik informatycznych, ASI informuje Dział Ekonomiczny (KE), który sporządza umowę powierzenia.
3. W przypadku konieczności powierzenia danych do przetwarzania w inny sposób niż określony w ust. 2, LADO informuje o tym fakcie Dział KE, który sporządza umowę powierzenia.
4. Treść umowy powierzenia uzgadniana jest z ABI.

§12

1. Dostęp do danych osobowych i ich przetwarzanie bez odrębnego upoważnienia ABI, może mieć miejsce wyłącznie w przypadku działań podmiotów upoważnionych na mocy odpowiednich przepisów prawa do dostępu i przetwarzania danych określonej kategorii.
2. W szczególności dostęp do danych osobowych na wskazanej w ust. 1 zasadzie, mogą mieć: Państwowa Inspekcja Pracy, Zakład Ubezpieczeń Społecznych, organy skarbowe, Policja, Agencja Bezpieczeństwa Wewnętrznego, Wojskowe Służby Informacyjne, sądy powszechne, Najwyższa Izba Kontroli, Generalny Inspektor Ochrony Danych Osobowych i inne upoważnione przez przepisy prawa podmioty i organy, działające w granicach przyznanych im uprawnień - po okazaniu dokumentów potwierdzających te uprawnienia.
3. Wszystkie kontrole przeprowadzane przez podmioty upoważnione na mocy odpowiednich przepisów prawa rejestrowane są w „Księdze Kontroli" znajdującej się w sekretariacie ADO.

§ 13

Instytut, realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych, zapewnia kontrolę nad dostępem do danych osobowych. Kontrola ta w szczególności sprawowana jest poprzez ewidencjonowanie osób przetwarzających dane osobowe oraz wdrożenie procedur udzielania dostępu do tych danych.

§ 14

1. Instytut zapewnia zaznajomienie osób upoważnionych do dostępu i/lub przetwarzania danych osobowych z powszechnie obowiązującymi przepisami prawa, uregulowaniami wewnętrznymi, a także technikami i środkami ochrony tych danych stosowanymi w Instytucie przed dopuszczeniem do pracy na stanowiskach związanych z przetwarzaniem danych osobowych, a także w trakcie trwania zatrudnienia – w przypadku zmian w obowiązujących przepisach prawa, uregulowaniach wewnętrznych lub technikach i środkach ochrony danych stosowanych w Instytucie.
2. Zaznajomienie, o którym mowa w ust. 1 może odbywać się w szczególności poprzez:
   a) instruktaż na stanowisku pracy,

b) szkolenie wewnętrzne przeprowadzone na terenie Instytutu,

c) szkolenie zewnętrzne.

§ 15

1. Instytut gwarantuje osobom fizycznym, których dane osobowe są przetwarzane w związku z realizacją jego celów statutowych, realizację uprawnień gwarantowanych im przez obowiązujące przepisy prawa.
2. W szczególności każdej osobie fizycznej, której dane osobowe są przetwarzane w związku z realizacją celów statutowych Instytutu, przysługuje prawo do uzyskania informacji o zakresie jej uprawnień związanych z ochroną danych osobowych, a także prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych na zasadach określonych w art. 32 - 35 Ustawy.
3. Osoby fizyczne, których dane osobowe są przetwarzane w związku z realizacją celów statutowych Instytutu, uzyskują informację o przysługujących im prawach.

§ 16

Naruszanie przez zatrudnione w ramach stosunku pracy osoby upoważnione do dostępu i/lub przetwarzania danych osobowych, zasad bezpiecznego i zgodnego z prawem ich przetwarzania, traktowane będzie jako ciężkie naruszenie podstawowych obowiązków pracowniczych z wszystkimi wynikającymi stąd konsekwencjami, z rozwiązaniem stosunku pracy włącznie.

§ 17

1. Celem zabezpieczenia zbioru danych osobowych przed dostępem osób nieupoważnionych wprowadza się w Instytucie odpowiednie rozwiązania techniczne i organizacyjne.
2. Zbiory danych osobowych chronione są nowoczesnymi mechanizmami szyfrowania.
3. W celu zabezpieczenia systemu informatycznego stosuje się zabezpieczenie firewall.
4. Dla zabezpieczenia zbioru danych osobowych przetwarzanych komputerowo stosuj się 8-znakowe hasło zmieniane co 30 dni.
5. Osoby nieupoważnione do przetwarzania danych osobowych określonej kategorii, mające interes prawny lub faktyczny w uzyskaniu dostępu do tych danych lub wykonujące inne czynności nie mające związku z dostępem do tych danych mogą przebywać w budynkach, pomieszczeniach i częściach pomieszczeń tworzących obszar Instytutu, w którym przetwarzane są dane osobowe podczas przetwarzania tych danych - wyłącznie w obecności upoważnionego pracownika Instytutu, lub – w razie jego nieobecności - na podstawie upoważnienia wydanego przez ABI.

§ 18

1. Całkowite opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe, musi wiązać się z zastosowaniem dostępnych środków zabezpieczających to pomieszczenie przed wejściem osób nieuprawnionych.
2. Opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe, musi wiązać się z zastosowaniem dostępnych środków zabezpieczających używane aktualnie zbiory danych osobowych. W szczególności w razie planowanej, choćby chwilowej, nieobecności pracownika upoważnionego do przetwarzana danych osobowych obowiązany jest on umieścić zbiory występujące w formach

tradycyjnych w odpowiednio zabezpieczonym miejscu ich przechowywania oraz dokonać niezbędnych operacji w systemie informatycznym uniemożliwiających dostęp do danych osobowych osobom nieuprawnionym.

3. Opuszczenie przez pracownika przetwarzającego dane osobowe obszaru ich przetwarzania bez zabezpieczenia budynku i/lub pomieszczenia oraz umiejscowionych w nim zbiorów danych jest niedopuszczalne i będzie uważane za naruszenie, o którym mowa w § 16.

§ 19

1. Dostęp do budynków i pomieszczeń Instytutu, w których przetwarzane są dane osobowe podlega kontroli. (Wykaz budynków, w których przetwarzane są dane osobowe w Instytucie oraz sposób ich zabezpieczenia stanowi załącznik nr 3 do Polityki).
2. Klucze do budynków i/lub pomieszczeń, w których przetwarzane są dane osobowe wydawane być mogą wyłącznie pracownikom upoważnionym do przetwarzania danych osobowych lub innym pracownikom upoważnionym do dostępu do tych budynków lub pomieszczeń.
3. Instytut, realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych, może wprowadzać inne formy monitorowania dostępu do obszarów przetwarzania danych osobowych.
4. Szczegółowe zasady kontroli dostępu do poszczególnych obszarów (budynków, pomieszczeń) Instytutu, w których przetwarzane są dane osobowe określane są przez osoby kierujące poszczególnymi komórkami organizacyjnymi Instytutu, w których takie obszary występują.

§ 20

1. W Instytucie sprawowana jest kontrola i nadzór nad niszczeniem zbędnych danych osobowych i/lub ich zbiorów.
2. Niszczenie zbędnych danych osobowych i/lub ich zbiorów polegać powinno w szczególności na:
   1) trwałym, fizycznym zniszczeniu danych osobowych i/lub ich zbiorów wraz z ich nośnikami w stopniu uniemożliwiającym ich późniejsze odtworzenie przez osoby nieuprawnione przy zastosowaniu powszechnie dostępnych metod;
   2) anonimizacji danych osobowych i/lub ich zbiorów, polegającej na pozbawieniu danych osobowych i/lub ich zbiorów, cech pozwalających na identyfikację osób fizycznych, których dane dotyczą.
3. Osoby przetwarzające dane osobowe w Instytucie mają obowiązek stosowania oddanych im do dyspozycji narzędzi i technik niszczenia zbędnych danych osobowych i/lub ich zbiorów.
4. Naruszanie przez osoby zatrudnione w Instytucie w ramach stosunku pracy, posiadające upoważnienie do dostępu i/lub przetwarzania danych osobowych, procedur niszczenia zbędnych danych osobowych i/lub ich zbiorów będzie uważane za naruszenie, o którym mowa w § 16.
5. Kontrola i nadzór nad niszczeniem zbędnych danych osobowych i/lub ich zbiorów może w szczególności polegać na wprowadzeniu odpowiednich procedur niszczenia danych, a także zlecaniu niszczenia ich wyspecjalizowanym podmiotom zewnętrznym, gwarantującym bezpieczeństwo procesu niszczenia danych odpowiednie do rodzaju nośnika tych danych.

6. Dane zarchiwizowane w archiwum Instytutu niszczone są zgodnie z procedurami określonymi w Instrukcji archiwalnej.

§ 21

1. Instytut, realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych, zapewnia, zgodną z przepisami rozdziału 5 Ustawy, ochronę zbiorom danych osobowych sporządzanym doraźnie, wyłącznie ze względów technicznych lub szkoleniowych, a po ich wykorzystaniu niezwłoczne usunięcie albo poddanie anonimizacji.
2. Osoby, które posiadają zbiory danych osobowych sporządzone doraźnie, dla nieistniejącego już celu (brak aktualnego upoważnienia), są zobowiązane do niezwłocznego usunięcia tych danych.

§ 22

Instytut, realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych zabrania tworzenia zbiorów danych osobowych, a także gromadzenia w zbiorach lub poza nimi kategorii danych osobowych innych niż niezbędne dla wykonania jego zadań statutowych.

§23

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiazania między nimi oraz sposób przepływów danych między poszczególnymi systemami stanowi załącznik nr 4 do niniejszej Polityki i dostępny jest w wersji papierowej w Dziale IP.

ZATWIERDZAM

DYREKTOR
dr inż. Adam Pietras

Załącznik nr 2
do Polityki Bezpieczeństwa

Gliwice, dnia.....

Upoważnienie
uprawniające do przetwarzania danych osobowych

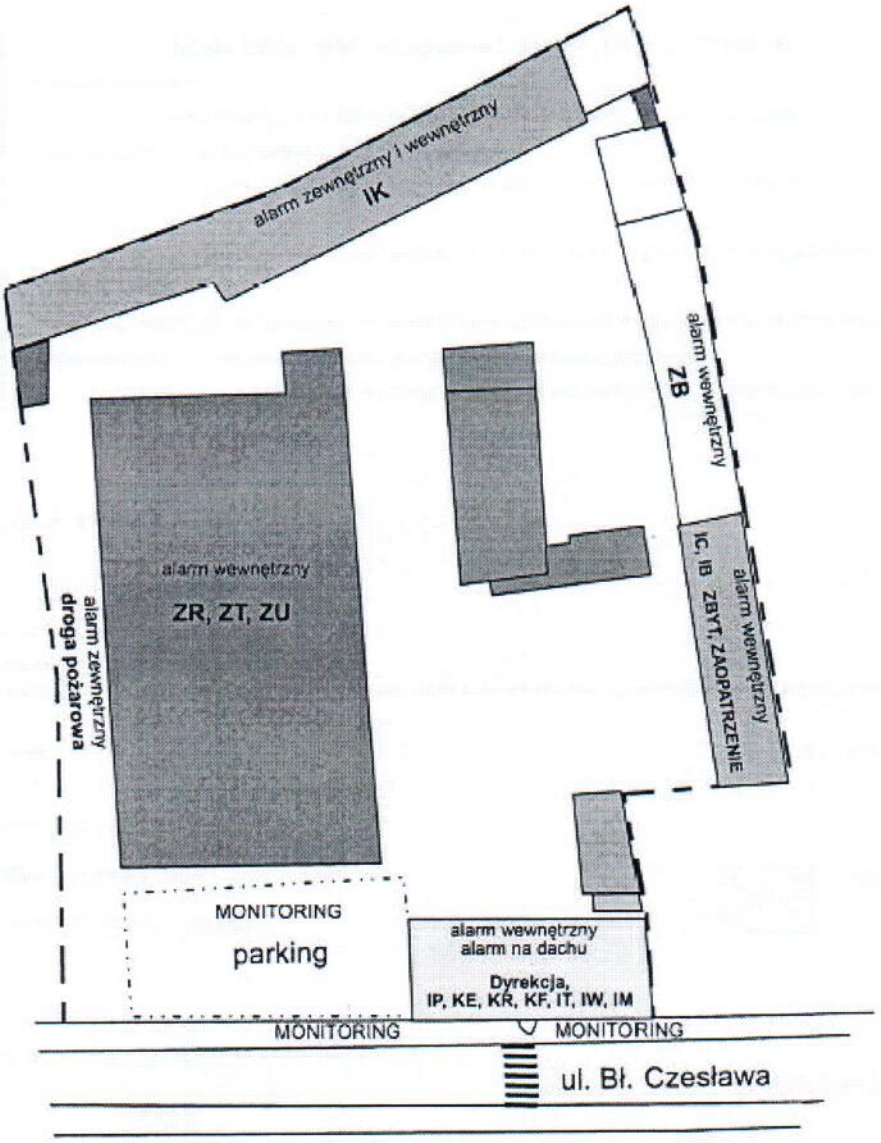
Niniejszym upoważniam Pana/Panią ..... do przetwarzania danych osobowych w zakresie wynikającym z powierzonych obowiązków wynikających z karty osobowej, która jest załącznikiem do niniejszego upoważnienia.

Pracownik oświadcza, że zapoznał się z postanowieniami Polityki bezpieczeństwa i Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, oraz, że jest mu znana treść ustawy o ochronie danych osobowych z dnia 29.08.1997 r. z późn. zm.

.....
Upoważniony

.....
Administrator Bezpieczeństwa Informacji

Załącznik nr 3
do Polityki Bezpieczeństwa

INSTYTUT SPAWALNICTWA

- zabezpieczenia budynków, w których przetwarzane są dane osobowe