POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH
Stowarzyszenia Inżynierów i Techników Przemysłu Chemicznego
Zarząd Główny w Warszawie

Stowarzyszenie Inżynierów i Techników Przemysłu Chemicznego, Zarząd Główny w Warszawie (zwany dalej ZG SITPChem), jako administrator przetwarzanych w nim danych osobowych jest zobowiązany do przestrzegania obowiązujących przepisów prawa w zakresie ich ochrony.

I. Postanowienia ogólne.

Art. 1

ZG SITPChem reprezentując Administratora Danych, wprowadza do stosowania dokument pod nazwą *Polityka Bezpieczeństwa Przetwarzania Danych Osobowych*, mając na względzie zapewnienie prawidłowej ochrony danych osobowych przetwarzanych w ZG, rozumianej jako ochronę danych przed ich udostępnieniem osobom nieupoważnionym, zmianą lub zabraniem przez osobę nieuprawnioną, utratą, uszkodzeniem lub zniszczeniem.

Polityka Bezpieczeństwa Przetwarzania Danych Osobowych została wydana zgodnie z:

- rozporządzeniem Parlamentu Europejskiego i Rady /UE/ 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE /Dz. Urz. UE.L nr 119, str.1/,
- ustawą z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz. U. z 2018 poz. 1000)
- rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Zmiana treści *Polityki Bezpieczeństwa Przetwarzania Danych Osobowych* wymaga zatwierdzenia przez Zarząd Główny.

Art. 2

Ilekroć w *Polityce Bezpieczeństwa* jest mowa o:

a) ***Ustawie*** – rozumie się przez to ustawę z dnia 10 maja 2018 roku o ochronie danych osobowych,

b) **RODO** – rozporządzenie Parlamentu Europejskiego i Rady /UE/ 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE /Dz. Urz. UE.L nr 119, str. 1/

c) ***Administratorze Danych(AD)*** – jest to organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania informacji, w tym danych osobowych. Administrator Danych może również przetwarzać dane powierzone mu przez innych Administratorów Danych. W ZG SITPChem, Administratora Danych reprezentuje Prezydium Zarządu Głównego

d) ***Zarząd*** – rozumie się przez to Zarząd Główny SITPChem (również oznaczany skrótowo ZG SITPChem)

e) ***Prezydium*** - rozumie się przez to Prezydium Zarządu Głównego SITPChem (również oznaczane skrótowo PZG SITPChem)

f) ***Osobie upoważnionej*** – czyli osobie posiadającej formalne upoważnienie wydane przez Administratora danych lub przez osobę wyznaczoną,

g) ***Osobie świadczącej pracę*** – pod pojęciem osoby świadczącej pracę w Oddziale rozumie się osobę wykonującą pracę na podstawie umowy cywilnoprawnej (umowa zlecenie, umowa o dzieło),

h) ***Procesor -*** osoba fizyczna, prawna, organ publiczny, jednostka lub inny podmiot zajmujący się przetwarzaniem danych osobowych, które powierzył mu Administrator

i) ***Odbiorcy –*** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe w oparciu m. in. o umowę powierzenia,

j) ***Danych osobowych*** – to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio poprzez powołanie się na numer identyfikacyjny (np. nr PESEL) albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. W szczególności za dane osobowe uważa się dane dotyczące adresu, wynagrodzenia, daty i miejsca urodzenia, stanu zdrowia, w połączeniu z imieniem i nazwiskiem lub numerem identyfikującym osobę np. numer PESEL, nr NIP itp.,

k) ***Przetwarzaniu danych osobowych*** – czyli jakiekolwiek operacjach wykonywanych na danych osobowych, takich jak:
   - odczyt – podgląd danych w formie elektronicznej i dokumentacji w formie papierowej
   - zbieranie – pozyskiwanie danych osobowych,
   - przechowywanie – przechowywanie w postaci papierowej lub elektroniczne
   - zmiana – zmiany w postaci papierowej
   - kopiowanie – wykonywanie kopii danych osobowych w formie elektronicznej, kserokopii i odpisów dokumentów w formie papierowej,
   - opracowywanie – wykonywanie operacji na danych osobowych – tworzenie raportów, opracowań, sprawozdań itp.
   - udostępnianie – udostępnianie uprawnionym podmiotom, instytucjom, organom
   - usuwanie – trwałe usunięcie danych osobowych w formie elektronicznej, zniszczenie danych osobowych w formie papierowej lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.

l) ***Zbiorze danych osobowych*** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie

m) ***Systemie informatycznym –*** zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych,

n) ***Systemie tradycyjnym*** – zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji oraz wyposażenie i środki trwałe wykorzystywane w celu przetwarzania danych osobowych na papierze,

o) ***Zabezpieczeniu danych w systemie informatycznym*** – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

Art. 3

Celem *Polityki Bezpieczeństwa* jest ochrona danych osobowych przetwarzanych w kartotekach, księgach, wykazach przechowywanych w Zarządzie Głównym w zakresie określonym ustawą i rozporządzeniem. Informacje te, są przetwarzane zarówno w postaci dokumentacji tradycyjnej, jak i elektronicznej.

Przez ochronę przetwarzanych danych osobowych należy rozumieć jako zapewnienie:

- poufności informacji – zapewnienie dostępu do danych wyłącznie uprawnionym osobom
- integralności informacji – zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania
- dostępność informacji – zapewnienie osobom upoważnionym dostępu do danych w wymaganym czasie i zakresie.

Politykę Bezpieczeństwa stosuje się w szczególności do:

- danych osobowych przetwarzanych w różnych systemach informatycznych: księgowych, edytorach tekstu itp.,
- wszystkich informacji dotyczących danych pracowników, zleceniobiorców, członków stowarzyszenia, sympatyków itp.,
- procesorów danych osobowych, którym przekazano dane osobowe do przetwarzania w oparciu o umowy powierzenia,
- informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
- rejestru osób trzecich mających upoważnienia Administratora Danych (AD) osobowych do przetwarzania danych osobowych,
- innych dokumentów zawierających dane osobowe.

Polityka Bezpieczeństwa Ochrony Danych Osobowych zawiera:

a) wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe
b) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych
c) sposób przepływu danych pomiędzy poszczególnymi systemami
d) środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Innymi dokumentami regulującymi ochronę danych osobowych w Zarządzie są:

- Ewidencja osób upoważnionych do przetwarzania danych osobowych
- Procedura postępowania w przypadku naruszenia ochrony danych osobowych

Art. 4

Do obowiązków ***Administratora Danych*** należy zrozumienie i zapewnienie świadomości bezpieczeństwa przetwarzania danych osobowych, jego problematyki oraz wymagań, a także organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami RODO i ustawy o ochronie danych osobowych.

Do obowiązków, należy również:

- podejmowanie odpowiednich i niezbędnych kroków mających na celu zapewnienie prawidłowej ochrony danych osobowych,
- wprowadzenie do stosowania procedur zapewniających prawidłowe przetwarzanie danych osobowych
- egzekwowanie stosowania środków bezpieczeństwa przetwarzania danych osobowych,
- poddawanie przeglądom skuteczność polityki bezpieczeństwa przetwarzanych danych osobowych
- zapewnienie podstaw prawnych do przetwarzania danych osobowych od chwili zebrania danych do chwili ich usunięcia,
- zapewnienie niezbędnych środków potrzebnych dla zapewnienia bezpieczeństwa przetwarzania danych osobowych.

Do obowiązków ***osób upoważnionych*** do przetwarzania danych osobowych należy znajomość, zrozumienie i stosowanie w możliwie największym zakresie wszelkich dostępnych środków ochrony danych osobowych oraz uniemożliwienie osobom nieuprawnionym dostępu do przetwarzanych dokumentów.

Do obowiązków, należy również:

- przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa oraz przyjętymi regulacjami,
- postępowania zgodnie z ustalonymi regulacjami wewnętrznymi dotyczącymi przetwarzania danych osobowych
- zbieranie danych osobowych dla oznaczonych, zgodnych z prawem celów i niepoddawaniem dalszemu przetwarzaniu niezgodnemu z tymi celami
- zachowania w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia.

I. **Wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe**

Art. 5

Przetwarzanie danych osobowych odbywa się wyłącznie w siedzibie Zarządu Głównego pod adresem Warszawa, ul. Tadeusza Czackiego 3/5.

Obszar przetwarzania danych osobowych obejmuje zamykane na klucz pomieszczenie biurowe na trzecim piętrze budynku, wynajmowane od Administratora budynku Naczelnej Organizacji Technicznej. W pomieszczeniu tym znajdują się szafy oraz szuflady zamykane na klucz, w których przechowywane są kartoteki, segregatory zawierające dane osobowe członków Zarządu Głównego, Prezydium Zarządu Głównego, jak również dane wszystkich Oddziałów Terenowych SITPChem oraz Zarządów tych Oddziałów Terenowych, których dane są przetwarzane m.in. w celu realizacji zadań statutowych.

I. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Art. 6

W Oddziale utworzono i wydzielono następujące zbiory danych osobowych:

a) ***zbiór danych członków Zarządu Głównego oraz Prezydium Zarządu Głównego (zbiór 1)*** – w którym przetwarzane są, w sposób tradycyjny (papierowo) oraz w formie elektronicznej dane: imię i nazwisko, data miejsce urodzenia, adres zamieszkania, telefon tytuł naukowy i (lub) zawodowy, specjalność naukowa lub zawodowa ukończone szkoły i uczelnie, stanowisko (deklaracje członkowskie), rachunek bankowy (wniosek o pożyczkę),
b) ***zbiór danych członków Zarządu Jednostek Organizacyjnych SITPChem, członków Prezydiów Zarządów tych Oddziałów oraz członków Jednostek Organizacyjnych SITPChem (Oddziałów) → (zbiór 2)*** – w którym przetwarzane są, w sposób tradycyjny (papierowo) oraz w formie elektronicznej dane: imię i nazwisko, data miejsce urodzenia, adres zamieszkania, telefon tytuł naukowy i (lub) zawodowy, specjalność naukowa lub zawodowa ukończone szkoły i uczelnie, stanowisko
c) ***zbiór danych uczestników różnych wyjazdów, spotkań, imprez, konferencji, sympozjum, kongresów, itp (zbiór 3)*** – w którym przetwarzane są w sposób tradycyjny oraz w formie elektronicznej następujące dane: imię i nazwisko, data urodzenia, adres nr telefonu, nr rachunku bankowego (karta zgłoszeniowa, zgłoszenie do ubezpieczenia NNW uczestników). W przypadku osoby

niepełnoletniej dodatkowo zamieszczone są dane prawnego opiekuna ww. osoby takie jak: imię i nazwisko, adres zamieszkania, telefon, stopień pokrewieństwa,

d) ***zbiór danych zawierających dokumentację księgową i pracowniczą (zbiór 4)*** – w których przetwarzane są w sposób tradycyjny (papierowo) oraz za pośrednictwem systemu informatycznego Płatnik następujące dane: imię i nazwisko, adres zamieszkania, data i miejsce urodzenia, PESEL, nr telefonu, nr rachunku bankowego (zatrudnienie osób świadczących pracę, zgłoszenie do ubezpieczeń).

e) ***zbiór danych osób przystępujących do egzaminu, uczestników szkoleń kursów, konferencji (zbiór 5)*** – w którym przetwarzane są w sposób tradycyjny następujące dane: imię i nazwisko, PESEL, nr telefonu (karta zgłoszeniowa).

I. Sposób przepływu danych pomiędzy poszczególnymi systemami

Art. 7

Zbiór 1 – dane ze zbioru udostępniane są członkom ZG i członkom PZG w celu realizacji zadań statutowych, jak również są udostępniane innym osobom lub organom, na podstawie ich pisemnej zgody na przetwarzanie danych osobowych lub w innych wypadkach prawem przewidzianych (art. 9 ust. 2d)

Zbiór 2 – dane ze zbioru udostępniane są członkom ZG i członkom PZG w celu realizacji zadań statutowych, jak również są udostępniane innym osobom lub organom, na podstawie ich pisemnej zgody na przetwarzanie danych osobowych lub w innych wypadkach prawem przewidzianych (art. 9 ust. 2d)

Zbiór 3 – dane ze zbioru udostępniane są członkom ZG oraz członkom PZG, jak również innym osobom m.in. realizatorom zadań, osobom świadczących pracę, procesorom w celu realizacji zadań statutowych. Uczestnictwo w spotkaniach, wyjazdach, imprezach, konferencjach, sympozjach, kongresach, itp., jest równoznaczne ze zgodą na przetwarzanie danych osobowych.

Zbiór 4 – dane ze zbioru są udostępniane członkom ZG i członkom PZG w celu realizacji zadań statutowych, jak również są udostępniane osobom świadczącym pracę w Oddziale, bankowi, w którym ZG posiada rachunek bankowy, ZUS, Urzędowi Skarbowemu oraz innym osobom lub organom, w wypadkach prawem przewidzianych lub na podstawie pisemnej umowy o powierzenie przetwarzania danych osobowych. Dane będą przechowywane przez okres 40 lat.

Zbiór 5 – dane ze zbioru udostępniane są Komisjom Egzaminacyjnym przy ZG w celu realizacji zadań statutowych, jak również są udostępniane innym instytucjom lub organom, na podstawie ich pisemnej zgody na przetwarzanie danych osobowych lub w innych wypadkach prawem przewidzianych (art. 9 ust. 2d)

I. Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Art. 8

Oddział realizując *Politykę Bezpieczeństwa* stosuje odpowiednie środki techniczne i organizacyjne zapewniające poufność, integralność danych osobowych gromadzonych i przetwarzanych w Oddziale.

Środki ochrony fizycznej przetwarzanych danych osobowych:

1) Klucze do pomieszczenia biurowego posiadają osoby upoważnione przez Administratora Danych
2) Przebywanie osób trzecich w pomieszczeniu gdzie są przetwarzane dane osobowe dopuszczalne jest tylko w obecności osoby upoważnionej do przetwarzania danych osobowych
3) Dokumentacja papierowa po godzinach pracy jest przechowywana w zamykanych szafach oraz szufladach. Klucze do szaf oraz szuflad przechowywane są w sejfie, do którego dostęp mają osoby upoważnione
4) Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone. Niszczenie zbędnych danych polega na trwałym, fizycznym zniszczeniu danych osobowych w stopniu uniemożliwiającym ich późniejsze odtworzenie przez osoby niepowołane przy zastosowaniu powszechnie dostępnych metod (niszczarki, spalenie itp.)

Środki sprzętowe, informatyczne i telekomunikacyjne:

1) Oprogramowanie antywirusowe działające na komputerze wykrywa i eliminuje wirusy, konie trojańskie oraz inne niebezpieczne oprogramowanie.
2) Dostęp do systemu operacyjnego komputera, w którym są przetwarzane dane osobowe jest zabezpieczony za pomocą procesu uwierzytelniania z wykorzystaniem identyfikatora użytkownika oraz hasła.
3) Obowiązuje zasada „czystego biurka i czystego ekranu” w celu redukcji ryzyka nieautoryzowanego i nieuprawnionego dostępu lub uszkodzenia danych osobowych.
4) Monitor komputera ustawiony jest w sposób uniemożliwiający podgląd wyświetlanych danych osobom postronnym.

Środki organizacyjne:

- Administrator Danych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, zawierającą w szczególności imię i nazwisko osoby upoważnionej, datę nadania i ustania uprawnień oraz zakres upoważnienia do przetwarzania danych osobowych *(Załącznik nr 1)*
- Do przetwarzania danych osobowych przetwarzanych przez Oddział mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora Danych. Wzór upoważnienia stanowi *Załącznik nr 2*. Cofnięcie upoważnienia do przetwarzania danych osobowych następuje każdorazowo w przypadku rozwiązania umowy z osobą świadczącą pracę czy umowy współpracy oraz zmiany zakresu odpowiedzialności osoby upoważnionej do przetwarzania danych na zakres niezwiązany z ich przetwarzaniem.
- Osoby upoważnione do przetwarzania danych osobowych zostają zaznajomione z powszechnie obowiązującymi przepisami prawa, uregulowaniami wewnętrznymi, a także zostają zobowiązane do zachowania w tajemnicy danych osobowych oraz stosowania przyjętych technik i środków ochrony tych danych. Osoby upoważnione do przetwarzania danych osobowych podpisują zobowiązanie do zachowania tajemnicy *(Załącznik nr 2).*
- Administrator Danych może powierzyć przetwarzanie danych osobowych innemu podmiotowi, w celu wykonania usług związanych z realizacją zadań statutowych Oddziału, ochroną osób i mienia, serwisowaniem systemu informatycznego, usług doradczych i in., zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO.
- Dostęp do danych osobowych bez upoważnienia może mieć miejsce wyłącznie w przypadku działań podmiotów upoważnionych na mocy odpowiednich przepisów prawa. Instytucja państwowa w przypadku wniesienia żądania udostępnienia danych osobowych przetwarzanych przez Zarząd Główny zobligowana jest do pisemnego wskazania podstawy prawnej do ich otrzymania oraz zakresu kontroli
- Stworzono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych *(Załącznik nr 4),*

I. **Prawa osób, których dane są przetwarzane przez Oddział**

Art. 9

Zgodnie z przepisami prawa w zakresie ochrony danych osobowych, przetwarzanie danych jest możliwe tylko wtedy, gdy:

a) osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych,
b) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,
c) jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
d) jest niezbędne do wykonania celów statutowych oraz określonych prawem zadań realizowanych dla dobra publicznego,
e) jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez Administratora Danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Wobec osoby, której dane dotyczą, wykonywany jest obowiązek informacyjny *(Załącznik nr 3)* zgodnie z treścią art. 13 i 14 RODO o:

a) adresie siedziby Administratora Danych,
b) celu zbierania danych,
c) nieudostępnianiu danych
d) prawie dostępu do treści swoich danych oraz ich poprawianiu,
e) dobrowolności lub obowiązku podania danych.

Art. 10

Zarząd Główny SITPChem gwarantuje osobom fizycznym, których dane osobowe są przetwarzane prawo do kontroli przetwarzania tych danych zgodnie z uprawnieniami gwarantowanymi im przez obowiązujące przepisy prawa, a zwłaszcza do:

a) uzyskania informacji, czy taki zbiór istnieje oraz do ustalenia Administratora Danych, adresu jego siedziby i pełnej nazwy,
b) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze,
c) uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, które dane te są udostępniane,
d) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one nieprawdziwe, nieaktualne lub zostały zebrane z naruszeniem przepisów prawa w zakresie ochrony danych osobowych albo są już zbędne do realizacji celu, dla którego zostały zebrane.

Art. 11

W przypadku stwierdzenia naruszenia ochrony danych osobowych Administrator Danych dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych. Administrator zgłasza fakt naruszenia zasad ochrony danych organowi nadzorczemu bez zbędnej zwłoki – jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. (Wzór zgłoszenia określa *Załącznik 4*). Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator zawiadamia o incydencie także osobę, której dane dotyczą.

I. Postanowienia końcowe

Art. 12

Niniejsza *Polityka Bezpieczeństwa* powinna być aktualizowana wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz zmianami faktycznymi w ramach Zarządu Głównego SITPChem, które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne.

Art. 13

Niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, naruszenie zasad określonych w niniejszej Polityce Bezpieczeństwa może być podstawą rozwiązania członkostwa/rozwiązania umowy na świadczenie pracy lub współpracy z osobą, która dopuściła się naruszenia.

W sprawach nieuregulowanych tym dokumentem zastosowanie mają odpowiednie przepisy aktów prawnych powszechnie obowiązujących.

Art. 14

Niniejszą *Politykę Bezpieczeństwa Przetwarzania Danych Osobowych* zatwierdzono Uchwałą Zarządu Głównego Stowarzyszenia Inżynierów i Techników Przemysłu Chemicznego w dniu: 04.11.2020 r.

Oryginał niniejszego dokumentu przechowywany jest w siedzibie Administratora Danych.

Warszawa, dnia 17.12. 2020 r.

Załącznik nr 1 – Rejestr wydanych upoważnień do przetwarzania danych osobowych

Lp.	Nr upoważnienia	Data wydania upoważnienia	Zakres czynności prawnych	Imię i nazwisko osoby otrzymującej

Załącznik nr 2 –

UPOWAŻNINIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) – dalej **RODO (GDPR),** niniejszym upoważniam do przetwarzania moich danych osobowych przez Stowarzyszenie Inżynierów i Techników Przemysłu Chemicznego w zakresie pełnionych obowiązków .....

Przetwarzanie danych osobowych będzie następowało na nośnikach papierowych i w systemach informatycznych (w tym zdjęcia)

Upoważniam Zarząd Główny SITPChem do przetwarzania danych osobowych zawartych w następujących zbiorach:

- zbiór danych członków Zarządu Głównego oraz Prezydium Zarządu Głównego **(zbiór 1)** – w którym przetwarzane są, w sposób tradycyjny (papierowo) oraz w formie elektronicznej dane: imię i nazwisko, data miejsce urodzenia, adres zamieszkania, telefon tytuł naukowy i (lub) zawodowy, specjalność naukowa lub zawodowa ukończone szkoły i uczelnie, stanowisko (deklaracje członkowskie), rachunek bankowy (wniosek o pożyczkę), → ☐
- zbiór danych członków Zarządu Jednostek Organizacyjnych SITPChem, członków Prezydiów Zarządów tych Oddziałów oraz członków Jednostek Organizacyjnych SITPChem (Oddziałów) → **(zbiór 2)** – w którym przetwarzane są, w sposób tradycyjny (papierowo) oraz w formie elektronicznej dane: imię i nazwisko, data miejsce urodzenia, adres zamieszkania, telefon tytuł naukowy i (lub) zawodowy, specjalność naukowa lub zawodowa ukończone szkoły i uczelnie, stanowisko → ☐
- zbiór danych uczestników różnych wyjazdów, wycieczek, spotkań, imprez, konferencji, sympozjum, kongresów, itp.--> **(zbiór 3)** – w którym przetwarzane są w sposób tradycyjny oraz w formie elektronicznej następujące dane: imię i nazwisko, data urodzenia, adres nr telefonu, nr rachunku bankowego (karta zgłoszeniowa, zgłoszenie do ubezpieczenia NNW uczestników), zdjęcia, filmy, nagrania głosowe. W przypadku osoby niepełnoletniej dodatkowo zamieszczone są dane prawnego opiekuna ww. osoby takie jak: imię i nazwisko, adres zamieszkania, telefon, stopień pokrewieństwa → ☐
- zbiór danych zawierających dokumentację księgową i pracowniczą → **(zbiór 4)** – w których przetwarzane są w sposób tradycyjny (papierowo) oraz za pośrednictwem systemu informatycznego Płatnik następujące dane: imię i nazwisko, adres zamieszkania, data i miejsce urodzenia, PESEL, nr telefonu, nr rachunku bankowego (zatrudnienie osób świadczących pracę, zgłoszenie do ubezpieczeń) → ☐
- zbiór danych osób przystępujących do egzaminu, uczestników szkoleń kursów, konferencji (**zbiór 5**) – w którym przetwarzane są w sposób tradycyjny następujące dane: imię i nazwisko, PESEL, nr telefonu (karta zgłoszeniowa). → ☐

Uwaga !! : należy wskazać zbiór 1, 2, 3, 4, 5 – przez zakreślenie znaku „x" w danej kratce

Upoważnienie obejmuje uprawnienie do przetwarzania danych w zakresie:

Niniejsze upoważnienie traci moc najpóźniej z dniem odwołania lub innej podstawy prawnej współpracy między osobą upoważnioną, a Zarządem Głównym lub Prezydium Zarządu Głównego Stowarzyszenia Inżynierów i Techników Przemysłu Chemicznego.

W imieniu Administratora Danych :

…… ……..

(Prezes Zarządu Głównego SITPChem) (Sekretarz Generalny Zarządu Głównego SITPChem)

Przyjąłem do wiadomości i jednocześnie zobowiązuję się do przestrzegania zasad zawartych w Polityce Bezpieczeństwa Przetwarzania Danych Osobowych ZG SITPChem

…… ……..……..

(data) *(czytelny podpis)*

Załącznik nr 3 –

……
(miejscowość i data)

OŚWIADCZENIE
o wyrażeniu zgody na gromadzenie i przetwarzanie danych osobowych

Wyrażam zgodę na gromadzenie i przetwarzanie moich danych osobowych przez Stowarzyszenie Inżynierów i Techników Przemysłu Chemicznego zgodnie na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) – dalej **RODO (GDPR),** dnia10 maja 2018 r. o ochronie danych osobowych w związku z :
- zgłoszeniem chęci skorzystania z : wyjazdu/ konferencji/ kongresu/ sympozjum /spotkania integracyjnego/wycieczką techniczną/
- realizowaną prezentacją/ wykładem/ posterem/ przemową/ artykułem w organizowanych spotkaniach/konferencjach/ kongresach/
- kursem/egzaminem organizowanym przez ZG SITPChem , PZG SITPChem bądź też, pozostałe Jednostki Organizacyjne SITPChem
- różnymi innymi działaniami statutowymi SITPChem

Jednocześnie oświadczam, że:

- zostałem zapoznany z klauzulą obowiązku informacyjnego zgodnie z art. 13 RODO
- wyrażam zgodę na prezentacje mojego wizerunku na materiałach zdjęciowych , filmowych, nagraniach, itp. w związku z uczestnictwem w różnego typu działalności SITPChem (kongresy, konferencje, postery, czasopisma, dzienniki, prezentacje, spotkania, wycieczki, uroczystości oficjalne, pogrzeby, spotkania integracyjne, itp.)
- przyjmuję do wiadomości, iż moje dane osobowe będą przetwarzane przez ZG i PZG SITPChem, w celach realizacji działań statutowych,
- podanie danych jest dobrowolne, aczkolwiek odmowa ich podania jest równoznaczna z brakiem możliwości skorzystania z naszej oferty,
- mam prawo dostępu do treści swoich danych i ich poprawienia.

…….. ……..
(miejscowość i data) (czytelny podpis uczestnika)

Załącznik 4 – Procedura postępowania w sytuacji naruszenia ochrony danych osobowych

Instrukcja postępowania
w sytuacji naruszenia ochrony danych osobowych

§ 1

Celem instrukcji jest ustalenie jednolitych zasad postępowania w przypadku, gdy:

- stwierdzono naruszenie lub istnieje podejrzenie naruszenia ochrony danych osobowych, zgromadzonych w systemach informatycznych lub na innych nośnikach informacji, w tym nośnikach papierowych,
- stan urządzenia, zawartość zbioru danych osobowych; ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zasad ochrony danych.

§ 2

Naruszenie ochrony danych osobowych może być skutkiem:

- zewnętrznych zdarzeń losowych,
- zamierzonych lub niezamierzonych czynności użytkowników systemów przetwarzania danych osobowych,
- nieuprawnionych działań osób nieupoważnionych do dostępu do danych osobowych.

§ 3

Za naruszenie zasad ochrony danych osobowych uważa się w szczególności:

- nieupoważniony dostęp, modyfikację, kopiowanie lub zniszczenie/usunięcie danych osobowych, zarówno w systemie informatycznym, jak i na nośnikach papierowych i elektronicznych,
- udostępnianie danych osobowych nieuprawnionym podmiotom lub osobom,
- nieautoryzowany dostęp do danych przez połączenie sieciowe,
- niedopełnienie obowiązku ochrony danych osobowych przez umożliwienie dostępu do danych (np. pozostawienie kopii danych, niezablokowanie dostępu do systemu, brak nadzoru nad osobami nieuprawnionymi przebywającymi w pomieszczeniach gdzie przetwarza się dane osobowe,

- wykrycie niezabezpieczonego kanału dystrybucji danych osobowych,
- nielegalne bądź nieświadome ujawnienie danych osobowych,
- pozyskiwanie danych osobowych z nielegalnych źródeł,
- przetwarzanie danych osobowych niezgodne z uprawnionym celem i zakresem,
- stwierdzenie obecności wirusów komputerowych lub innych programów godzących w integralność systemu informatycznego,
- ujawnienie indywidualnych haseł dostępu do danych osobowych w systemie,
- przesyłanie danych osobowych przez Internet bez zabezpieczenia,
- przesyłanie dokumentów papierowych i nośników elektronicznych z danymi bez zabezpieczenia,
- wykonanie nieuprawnionych kopii danych osobowych,
- naruszenie bezpieczeństwa kopii danych osobowych,
- kradzież nośników zawierających dane osobowe lub oprogramowanie,
- kradzież sprzętu służącego do przetwarzania danych osobowych,
- utratę danych osobowych w systemie informatycznym, na kopiach bezpieczeństwa i na innych nośnikach,
- brak aktualnych kopii bezpieczeństwa danych osobowych lub brak odpowiednich nośników do sporządzania kopii,
- niewłaściwe niszczenie nośników z danymi osobowymi pozwalające na ich odczyt,
- naruszenie zasad ochrony fizycznej pomieszczeń, w których przetwarza się dane osobowe.
- dopuszczenie do przetwarzania danych osobowych pracowników bez odpowiednich upoważnień.
- nie przeszkolenie pracowników w zakresie bezpieczeństwa danych osobowych
- inne sytuacje wskazujące lub potwierdzające naruszenie bezpieczeństwa danych osobowych

§ 4

O możliwości zaistnienia przypadku naruszenia zasad ochrony danych osobowych mogą świadczyć m.in.:

- nadmierne, w stosunku do wykonywanych zadań, uprawnienia użytkownika do zasobów systemu,
- zanotowanie w krótkim czasie dużej liczby nieudanych prób logowania
- anomalie w pracy systemu lub programu (świadczące np. o obecności wirusa),
- naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach, w których przetwarza się dane osobowe (wyłamane lub zacinające się zamki, naruszone plomby, niedomykające się okna itp.),

§ 5

Osoba, która podejrzewa lub stwierdzi naruszenie zasad ochrony danych osobowych ma obowiązek niezwłocznie (bezpośrednio lub telefonicznie):

- powiadomić o zaistniałym zdarzeniu Administratora danych osobowych
- określić symptomy świadczące o możliwości naruszenia lub naruszeniu zasad ochrony danych,
- określić sytuację i czas w jakim je zauważono,
- podać wszelkie istotne informacje mogące pomóc w ustaleniu przyczyny naruszenia zasad ochrony danych osobowych,
- nie podejmować dalszej pracy w systemie informatycznym bez decyzji Administratora.

§ 6

Administrator danych osobowych ocenia sytuację i podejmuje odpowiednie do potrzeb działania, a w szczególności:

- dokonuje rozpoznania zdarzenia,
- ocenia wagę problemu,
- ocenia możliwość wystąpienia strat w zasobach informacyjnych i systemowych w przypadku dalszego działania systemu,
- lokalizuje źródło problemu (przeprowadza analizę posiadanych danych).

§7

W przypadku stwierdzenia, że podejrzenie nie świadczy o naruszeniu zasad ochrony danych, Administrator danych osobowych po przeanalizowaniu sytuacji i wyeliminowaniu możliwości wystąpienia ich w przyszłości, podejmuje decyzję o dalszej pracy systemu.

§ 8

W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Urzędowi ochrony danych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:
a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

- Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.
- Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

§ 9

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w § 10 ust. 2 lit. b), c) i d).

Zawiadomienie, o którym mowa wyżej, nie jest wymagane, w następujących przypadkach:

a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;

c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

§ 10

Każda osoba dopuszczona do przetwarzania danych osobowych obowiązana jest zapoznać się z niniejszą Instrukcją oraz złożyć stosowne oświadczenie dotyczące znajomości wymienionych regulacji.

Poświadczam znajomość „**Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych:**

Lp.	Data	Imię i nazwisko	Podpis