Centro-Chem Sp. z o.o. Sp.k.

POLITYKA OCHRONY DANYCH OSOBOWYCH

w spółce Centro-Chem Sp. z o.o. Sp.k. z siedzibą w Turce

Turka 2025

Spis treści

Wstęp

Centro-Chem spółka z ograniczoną odpowiedzialnością Spółka komandytowa w Turce, Turka 141B, 20-258 Lublin, wpisaną do Rejestru Przedsiębiorców pod numerem KRS: 0000822639, NIP: 7132339236, REGON: 43093238600000, zwana dalej „Centro-chem sp. z o.o. sp.k" lub „Spółka", szanuje prywatność osób, których dane przetwarza oraz dokłada najwyższej staranności, aby dane te były przetwarzane zgodnie z prawem oraz międzynarodowymi zasadami dobrych praktyk. Spółka dokłada szczególnych starań w celu ochrony prywatności i przekazanych jej informacji, z należytą starannością dobiera i stosuje odpowiednie środki techniczne, w tym o charakterze informatycznym i organizacyjnym zapewniające ochronę przetwarzanych danych, w szczególności zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym, ujawnieniem, utraceniem i zniszczeniem, nieuprawnioną modyfikacją, jak również przed ich przetwarzaniem z naruszeniem obowiązujących przepisów prawa.

Niniejsza Polityka Ochrony Danych Osobowych, zwana dalej Polityką, została sporządzona w celu wykazania, że dane osobowe są przetwarzane i zabezpieczone zgodnie z wymogami prawa, dotyczącymi zasad przetwarzania i zabezpieczenia danych w Centro-chem sp. z o.o. sp.k, zwanego dalej: „Administratorem", w szczególności przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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)[1], ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[2], a także innych aktów prawnych, które znajdują zastosowanie do przetwarzania danych osobowych i ochrony prywatności.

W celu zapewnienia ochrony prywatności osób, których dane dotyczą Centro-chem sp. z o.o. sp.k stosuje ścisłe zabezpieczenia wewnętrzne oraz zewnętrzne. Centro-chem sp. z o.o. sp.k, jako Administrator danych osobowych sprawuje stałą kontrolę nad procesem przetwarzania danych oraz ogranicza dostęp do danych w możliwie największym stopniu, udzielając stosownych upoważnień tylko wówczas, gdy jest to niezbędne do prawidłowego przetwarzania danych osobowych.

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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 119, s. 1)

[2] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2019 poz. 1781)

Rozdział I

Postanowienia ogólne

§ 1

1. Ilekroć w dalszej części niniejszej Polityki jest mowa bez bliższego określenia o:
    1) Administratorze (ADO) – należy przez to rozumieć administratora danych osobowych Spółkę należy przez to rozumieć Spółkę Centro-Chem spółka z ograniczoną odpowiedzialnością spółka komandytowa, Turka 141B, 20-258 Lublin; wpisaną do Rejestru Przedsiębiorców pod numerem KRS: 0000822639, NIP: 7132339236, REGON: 43093238600000;
    2) Anonimizacji danych osobowych – należy przez to rozumieć pozbawienie danych osobowych cech pozwalających na identyfikacje osób fizycznych, których te dane dotyczą;
    3) Bazie danych osobowych – należy przez to rozumieć zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci wewnętrznej czy zewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze - rekordów lub obiektów, w których są zapisane dane osobowe;
    4) Bezpieczeństwie informacji – należy przez to rozumieć zapewnienie poufności, integralności i dostępności przetwarzanych danych osobowych.
    5) Danych osobowych – należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
    6) Danych osobowych szczególnych – należy przez to rozumieć dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby. **Załącznik nr 2** stanowi wzór do niniejszej Polityki;
    7) Danych osobowych zwykłych – należy przez to rozumieć wszystkie dane osobowe nie stanowiące danych osobowych szczególnych. **Załącznik nr 1** stanowi wzór do niniejszej Polityki;
    8) Dostępności – należy przez to rozumieć gwarancję dostępu do danych osobowych tylko przez osoby upoważnione;
    9) Haśle – należy przez to rozumieć ciąg 9 znaków literowych, cyfrowych i innych specjalnych znanych jedynie osobie uprawnionej do pracy w systemie informatycznym. Hasło musi składać się z przynajmniej: jednej dużej, jednej małej litery, jednej cyfry i jednego znaku specjalnego;

10) Identyfikatorze użytkownika – należy przez to rozumieć ciąg znaków literowych, cyfrowych lub innych specjalnych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych w systemie informatycznym;
11) Incydencie – należy przez to rozumieć naruszenie ochrony danych osobowych;
12) Integralności danych – należy przez to rozumieć właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany (przez osoby nieupoważnione);
13) Loginie (identyfikatorze) – należy przez to rozumieć ciąg znaków alfanumerycznych, unikalnych dla każdego użytkownika korzystającego z zasobów informatycznych przetwarzanych i gromadzonych na serwerze lub w programie sieci informatycznej;
14) Inspektorze Ochrony Danych (IOD) – należy przez to rozumieć osobę formalnie powołaną przez Administratora, zobowiązaną do: informowania Administratora, Procesora oraz Pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy odpowiednich przepisów o ochronie danych i doradzanie im w tej sprawie; monitorowania przestrzegania przepisów o ochronie danych oraz polityki Administratora lub Procesora w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty; udzielania informacji co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania.
15) Naruszeniu ochrony danych osobowych – należy przez to rozumieć przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych, przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
16) Obszarze przetwarzania – należy przez to rozumieć pomieszczenia lub część pomieszczeń biurowych, tworzących obszar, w których Spółka lub pracownicy Spółki przetwarzają dane osobowe;
17) Ograniczeniu przetwarzania – należy przez to rozumieć oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
18) Organie nadzorczym – należy przez to rozumieć Prezes Urzędu Ochrony Danych Osobowych, zwany dalej PUODO, lub ewentualnie właściwy organ nadzorczy w zakresie danych osobowych wyznaczony przez inne państwo członkowie Unii Europejskiej;
19) Osobie nieupoważnionej – należy przez to rozumieć osoba nie posiadająca upoważnienia do przetworzenia danych osobowych nadanego przez Administratora Danych Osobowych;,

20) Poufności – należy przez to rozumieć właściwość zapewniającą, że dane nie są udostępniane;
21) Podmiocie danych – należy przez to rozumieć osobę fizyczną, której dotyczą dane osobowe przetwarzane przez Administratora;
22) Podmiocie przetwarzający – należy przez to rozumieć oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;
23) Poufności danych – należy przez to rozumieć właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
24) Polityce – należy przez to rozumieć niniejszą Politykę Ochrony Danych Osobowych, która zawiera w szczególności zestaw technicznych i organizacyjnych środków ochrony danych osobowych wprowadzonych, wdrożonych i stosowanych w Centro-chem sp. z o.o. sp.k niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych opisanych w niniejszym dokumencie;
25) Polityce Bezpieczeństwa Informacji Systemów IT – należy przez to rozumieć Politykę Bezpieczeństwa Informacji Systemów IT obowiązującą w Centro-chem sp. z o.o. sp.k;
26) Pracowniku – należy przez to rozumieć osoba fizyczna zatrudniona przez Administratora na podstawie umowy o pracę;
27) Procesie przetwarzania danych – należy przez to rozumieć zespół czynności przetwarzania danych osobowych;
28) Profilowaniu – należy przez to rozumieć dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
29) Przetwarzaniu danych – należy przez to rozumieć jakiekolwiek operacje wykonywane na Danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie w formie tradycyjnej oraz w systemach informatycznych;
30) Rejestrze czynności przetwarzania – należy przez to rozumieć dokument, który ma pokazywać w szczególności w jakich procesach w Centro-chem sp. z o.o. sp.k są przetwarzane dane osobowe, w jakim celu, kogo dotyczą oraz jak są zabezpieczane. Dokument ten będzie musiał zostać udostępniony na każde wezwanie PUODO;
31) Rozliczalności – należy przez to rozumieć właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

32) Rozporządzeniu – należy przez to rozumieć Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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 „RODO");
33) Sieci informatycznej – należy przez to rozumieć struktura składająca się z serwerów, stacji roboczych, osprzętu sieciowego, połączonych ze sobą za pomocą mediów transmisji w celu wymiany danych lub współdzielenia różnych zasobów;
34) Stacji roboczej – należy przez to rozumieć stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego, umożliwiający Użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie;
35) Systemie informatycznym – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji, narzędzi programowych zastosowanych w celu przetwarzania danych;
36) Systemie tradycyjny – należy przez to rozumieć zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji, wyposażenia i środków trwałych w celu przetwarzania danych osobowych w formie papierowej;
37) Usuwaniu danych – należy przez to rozumieć zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą (anonimizacja danych);
38) Ustawie – należy przez to rozumieć ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych;
39) Uwierzytelnianiu – należy przez to rozumieć działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
40) Użytkowniku – należy przez to rozumieć osobę upoważniona przez Administratora do przetwarzania danych osobowych;
41) Współadministrowaniu – należy przez to rozumieć sytuację w której co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania danych;
42) Współpracowniku – należy przez to rozumieć osoba fizyczna świadcząca na rzecz Administratora usługi na podstawie umowy cywilnoprawnej (np. umowa zlecenie, umowa o dzieło);
43) Zabezpieczeniu danych w systemie informatycznym – należy przez to rozumieć wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, mające na celu w szczególności zabezpieczenie danych przed ich udostępnianiem osobom nieupoważnionym. zabraniem przez osobę nieuprawnioną, zmianą, utratą, uszkodzeniem lub zniszczeniem;

44) Zbiorze danych osobowych – należy przez to rozumieć każdy posiadający strukturę zestaw danych o charakterze osobowym dostępnych według określonych kryteriów niezależnie od jego rozproszenia czy podziału;
45) Zdarzeniu – należy przez to rozumieć informacja lub okoliczność dająca podejrzenie naruszenia ochrony danych osobowych na podstawie, której dokonuje się oceny ryzyka naruszenia praw i wolności. W przypadku stwierdzenia braku zagrożenia dla praw i wolności zdarzenie nie stanowi naruszenia tych praw;
46) Zgodzie osoby, której dane dotyczą – należy przez to rozumieć oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

2. Polityka obowiązuje wszystkich pracowników Centro-chem sp. z o.o. sp.k, w tym również stażystów, wolontariuszy, praktykantów oraz dostawców, podmioty współpracujące na podstawie umów cywilnoprawnych, mające jakikolwiek kontakt z danymi osobowymi objętymi ochroną.
3. Polityka dotyczy wszystkich Danych osobowych przetwarzanych w Centro-chem sp. z o.o. sp.k niezależnie od formy ich przetwarzania (przetwarzane tradycyjnie, zbiory ewidencyjne, systemy informatyczne) oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych.
4. Polityka jest przechowywana w wersji elektronicznej oraz w wersji papierowej w siedzibie Administratora.
5. Jednobrzmiąca z pisemną elektroniczna forma niniejsza Polityka jest udostępniania Podmiotom przetwarzającym i Użytkownikom, w celu zapoznania z zasadami przetwarzania i zabezpieczania Danych osobowych wykorzystywanych w ramach działalności przedsiębiorstwa prowadzonego przez Administratora danych.
6. Dla skutecznej realizacji Polityki Administrator Danych zapewnia:
    1) odpowiednie do zagrożeń i kategorii danych objętych ochroną środki techniczne i rozwiązania organizacyjne;
    2) kontrolę i nadzór nad Przetwarzaniem danych osobowych,
    3) monitorowanie zastosowanych środków ochrony.
7. Monitorowanie przez Administratora Danych zastosowanych środków ochrony obejmuje m.in. działania Użytkowników, naruszanie zasad dostępu do danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.
8. Administrator Danych zapewnia, że czynności wykonywane w związku z przetwarzaniem i zabezpieczeniem danych osobowych są zgodne z niniejszą polityką oraz odpowiednimi przepisami prawa.

9. W przypadku współpracy z podmiotem trzecim obejmującej przetwarzanie danych osobowych na zlecenie Administratora, Spółka zapewnia, by taki podmiot trzeci zobowiązał się do zapewnienia odpowiedniego poziomu ochrony danych osobowych, z uwzględnieniem postanowień Polityki.
10. W przypadku współpracy z podmiotem trzecim, obejmującej przetwarzanie przez Administratora danych osobowych na zlecenie tego podmiotu, Spółka zawiera umowę powierzenia przetwarzania danych osobowych oraz zapewnia stosowanie się do jej wymogów przez wszystkie osoby zaangażowane w tę współpracę.
11. Administrator poprzez odpowiednie środki techniczne i organizacyjne zapewnia możliwość wykazania zgodności przetwarzania danych osobowych z RODO oraz pozostałymi przepisami dotyczącymi danych osobowych („rozliczalność").
12. Powołując IOD Administrator zapewnia, by odpowiadał on bezpośrednio przed zarządem Administratora, oraz dba o unikanie konfliktu interesów pomiędzy IOD a Spółką.
13. Wdrożenie Polityki ma na celu zapewnienie zgodności z RODO procesów przetwarzania przez Administratora danych osobowych, bez względu na formę (elektroniczną bądź papierową), w jakiej to przetwarzanie następuje.

§ 2.

Cele, założenia i zakres stosowania Polityki ochrony danych osobowych

1. Polityka stanowi zbiór zasad obowiązujących przy przetwarzaniu danych osobowych w Centro-chem sp. z o.o. sp.k.
2. Polityka składa się z:
    1) opisu zasad ochrony danych osobowych, obowiązujących u Administratora;
    2) załączników uszczegóławiających i uzupełniających niniejszą Politykę.
3. Celem Polityki jest:
    1) zapewnienie właściwego poziomu bezpieczeństwa danych osobowych w Centro-chem sp. z o.o. sp.k poprzez wdrożenie odpowiedniego systemu ich ochrony przed zagrożeniami wewnętrznymi i zewnętrznymi;
    2) podniesienie poziomu świadomości pracowników Centro-chem sp. z o.o. sp.k co do istoty problemu bezpieczeństwa danych osobowych.
4. W celu wdrożenia i realizacji Polityki Administrator zapewnia:
    1) odpowiednie do zagrożeń i kategorii Danych objętych ochroną środki techniczne i rozwiązania organizacyjne;
    2) kontrolę i nadzór nad Przetwarzaniem Danych osobowych;
    3) monitorowanie zastosowanych środków ochrony.
5. Ochrona danych osobowych u Administratora opiera się na następujących założeniach:
    1) **Zgodności z prawem** − Administrator dba o ochronę prywatności i przetwarza dane zgodnie z prawem;

2) **Bezpieczeństwa** – Administrator dokłada wszelkich starań, aby zapewnić odpowiedni poziom bezpieczeństwa danych;
3) **Praw osób, których dane dotyczą** – Administrator umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje;
4) **Rozliczalności** – Administrator dokumentuje to, w jaki sposób wywiązuje się z ciążących na nim obowiązków ochrony danych osobowych, aby w każdej chwili móc wykazać zgodność przetwarzania danych osobowych z RODO.

6. Administrator przetwarza dane osobowe z poszanowaniem następujących zasad:
   1) **Zgodności z prawem** – dane osobowe przetwarzane są w oparciu o konkretną podstawę prawną i zgodnie z prawem;
   2) **Rzetelności** – dane osobowe przetwarzane są rzetelnie i uczciwie;
   3) **Przejrzystości** – dane osobowe przetwarzane są w sposób przejrzysty dla osoby, której dane dotyczą;
   4) **Minimalizacji** – dane osobowe przetwarzane są wyłącznie w zakresie niezbędnym do celów;
   5) **Adekwatności** – przetwarzanie danych osobowych jest proporcjonalne do potrzeb Administratora;
   6) **Ograniczoności przechowywania** – dane są przechowywane przez Administratora przez okres nie dłuższy niż niezbędne jest to do celów, w których dane te są przetwarzane;
   7) **Prawidłowości** – przetwarzanie danych osobowych odbywa się z dbałością o prawidłowość danych osobowych;
   8) **Czasowości** – przetwarzanie danych osobowych odbywa się w koniecznym czasie;
   9) **Integralności i poufności** – Administrator zapewnia odpowiednie bezpieczeństwo przetwarzania danych osobowych.
7. Zasady określone przez Politykę mają zastosowanie do wszystkich zbiorów danych osobowych administrowanych przez Administratora, w szczególności do:
   1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są lub będą dane osobowe podlegające ochronie;
   2) danych osobowych przetwarzanych przez Administratora zarówno w przypadku, gdy jest on administratorem danych, jak i w sytuacji, gdy przetwarza dane powierzone mu na podstawie umów powierzenia przetwarzania danych osobowych, w rozumieniu art. 28 RODO;
   3) wszystkich nośników informacji, np. papierowych, magnetycznych, optycznych itp., na których są lub będą znajdować się dane osobowe podlegające ochronie;

4) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane dane osobowe podlegające ochronie;
5) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, konsultantów, stażystów i innych osób mających dostęp do danych osobowych podlegających ochronie.

Rozdział II

Organizacja Przetwarzania Danych Osobowych

§ 3.

1. Podmiotem odpowiedzialnym za przetwarzanie danych jest administrator i to on deleguje obowiązki inspektorowi ochrony danych (jeśli został powołany) oraz swoim pracownikom. Na administratorze ciąży odpowiedzialność prawna za wywiązanie się ze swoich obowiązków w związku z przetwarzaniem danych osobowych przez niego samego lub w jego imieniu. Podstawowym obowiązkiem administratora jest dbanie o to aby przetwarzanie odbywało się zgodnie z rozporządzeniem RODO i aby móc to wykazać. W tym celu, ma on wdrażać odpowiednie i skuteczne środki techniczne i organizacyjne:
    1) mają one zapewniać najwyższy znany i możliwy w chwili przetwarzania danych, poziom ochrony;
    2) nie może być to czynność jednorazowa, środki te są w razie potrzeby poddawane przeglądom i uaktualniane;
    3) dokonuje on tego, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia;
    4) środki te obejmują wdrożenie przez administratora polityki ochrony danych.
2. Administrator jest zobowiązany przez RODO do:
    1) wskazania podstawy prawnej do legalnego przetwarzania danych osobowych;
    2) zabezpieczenia przetwarzanych danych osobowych przed ich udostępnieniem osobom nieupoważnionym oraz zabraniem przez osobę nieuprawnioną;
    3) przetwarzania danych zgodnie z wymogami RODO;
    4) chronienia danych przed zmianą, utratą, uszkodzeniem lub zniszczeniem.
3. Zadania te powinny zostać zrealizowane poprzez:
    1) opracowanie dokumentacji;
    2) prowadzenie ewidencje osób upoważnionych do przetwarzania danych osobowych - **załącznik nr 3** do niniejszej Polityki, w tym również stażystów, wolontariuszy, praktykantów, uczniów przetwarzających dane w Spółce;
    3) monitorowanie czynności wykonywanych na zbiorze danych;
    4) zapewnienie technicznych środków bezpieczeństwa.

4. Odnośnie obowiązku informacyjnego, administrator danych:
    1) prowadzi komunikację z podmiotami danych (osobami fizycznymi) i przekazuje im informacje w sposób zwięzły, przejrzysty, zrozumiały i łatwo dostępny;
    2) ułatwia podmiotom danych wykonywanie ich praw;
    3) nieodpłatnie udziela podmiotom danych informacji, również na ich żądanie, czas na udzielenie informacji przez ADO to maksymalnie miesiąc; w sytuacjach skomplikowanych okres ten może zostać wydłużony do dwóch miesięcy,
    4) weryfikuje tożsamość osób wnoszących żądania udzielenia informacji.
5. Odnośnie praw osoby, której dane dotyczą:
    1) ADO potwierdza czy przetwarzane są dane osobowe dotyczące danej osoby fizycznej, a jeżeli ma to miejsce, udziela wskazanych rozporządzeniem informacji;
    2) ułatwia osobie, której dane dotyczą wykonywanie jej praw z art. 15–22 RODO;
    3) informuje osobę, której dane dotyczą, o działaniach jakie podjął, w związku z jej żądaniami opartymi o art. 15-22 RODO;
    4) uzasadnienia odrzucenie żądania osoby, której dane dotyczą i poucza ją o prawie skargi;
    5) umożliwia dostęp do jej danych osobie, której one dotyczą;
    6) dokonuje sprostowania i uzupełniane danych;
    7) usuwa dane;
    8) ogranicza przetwarzanie danych;
    9) powiadamia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu ich przetwarzania;
    10) dokonuje przenoszenia danych.

§ 4.

1. Administrator przypisuje role i zakres odpowiedzialności w procesie przetwarzania danych każdemu z uczestników tego procesu.
2. Przed udzieleniem dostępu do przetwarzania danych osobowych Administrator zapoznaje każdego Pracownika, Współpracownika lub inne osoby przetwarzające dane z jego upoważnienia, z procedurami i zasadami dotyczącymi ochrony danych osobowych obowiązującymi u Administratora.
3. Przetwarzanie danych osobowych przez Pracowników i Współpracowników może odbywać się wyłącznie na podstawie udokumentowanego upoważnienia Administratora, którego zakres odpowiada przypisanej roli i zakresowi odpowiedzialności. Ponadto Administrator zobowiązuje osoby upoważnione do zachowania poufności danych oraz informacji dotyczących zabezpieczeń danych, a także do przestrzegania procedur i polityk dotyczących ochrony danych obowiązujących w organizacji Administratora.
4. Administrator dokonuje identyfikacji zasobów danych osobowych, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych, w szczególności:

przypadków przetwarzania danych wrażliwych, przypadków przetwarzania danych niezidentyfikowanych, profilowania.

5. Administrator weryfikuje czy dochodzi do przypadków współadministrowania danymi osobowymi.
6. Dane osobowe przetwarzane przez Administratora Danych gromadzone są w zbiorach danych.
7. Administrator danych nie podejmuje czynności przetwarzania, które mogłyby się wiązać z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka dla praw i wolności osób. W przypadku planowania takiego działania Administrator wykona czynności określone w art. 35 i nast. RODO.
8. W przypadku planowania nowych czynności przetwarzania Administrator dokonuje analizy ich skutków dla ochrony danych osobowych oraz uwzględnia kwestie ochrony danych w fazie ich projektowania.

§ 5

1. Administrator prowadzi Rejestr Czynności Przetwarzania Danych Osobowych, zwany dalej: Rejestrem, który stanowi **załącznik nr 4** do niniejszej Polityki.
2. W Rejestrze, dla każdej czynności przetwarzania danych, którą Administrator uznał za odrębną dla potrzeb Rejestru, odnotowuje co najmniej:
    a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;
    b) nazwę czynności,
    c) cel przetwarzania,
    d) opis kategorii osób,
    e) opis kategorii danych,
    f) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu Administratora, jeśli podstawą jest uzasadniony interes,
    g) sposób zbierania danych,
    h) opis kategorii odbiorców danych (w tym przetwarzających),
    i) informację o przekazaniu poza EU/EOG;
    j) ogólny opis technicznych i organizacyjnych środków ochrony danych.
3. Wzór Rejestru zawiera kolumny nieobowiązkowe. W kolumnach nieobowiązkowych rejestruje się informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść Rejestru ułatwia zarządzanie zgodnością ochrony danych osobowych.
4. Rejestr czynności przetwarzania danych osobowych prowadzony jest w formie pisemnej oraz elektronicznej i uaktualniany na bieżąco przez Inspektora Ochrony Danych.

5. Rejestr Czynności Przetwarzania Danych Osobowych określa zakres danych osobowych, do których przetwarzania został upoważniony pracownik ADO. Powyższy zakres jest zależny od stanowiska, na którym zatrudniony jest pracownik ADO.
6. Inspektor Ochrony Danych lub ADO zapoznaje pracownika z Rejestrem Czynności Przetwarzania Danych Osobowych wyłącznie w zakresie czynności przetwarzania danych, do których pracownik ADO jest upoważniony do przetwarzania.

§ 6

1. ADO prowadzi Rejestr Kategorii Przetwarzania Danych.
2. Wzór rejestru, o którym mowa w ust. 1, stanowi **załącznik nr 5** do niniejszej Polityki.
3. W Rejestrze, o którym mowa w ust. 1, zamieszcza się m.in. następujące informacje:
    1) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;
    2) kategorie przetwarzań;
    3) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe);
    4) nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane;
    5) dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi RODO.
4. Rejestr Kategorii Przetwarzania Danych prowadzony jest w formie pisemnej oraz elektronicznej i uaktualniany na bieżąco przez Inspektora Ochrony Danych

§ 7

1. ADO stosuje odpowiednie środki informatyczne, techniczne, zapewniające ochronę przetwarzanych danych osobowych, które są odpowiednie do stopnia zagrożeń oraz kategorii danych objętych ochroną.
2. ADO stosuje następujące środki techniczne:
    a) przetwarzanie danych osobowych następuje w pomieszczeniach odpowiednio zabezpieczonych i przystosowanych do przetwarzania;
    b) pomieszczenia zabezpieczone są systemem monitorującym i alarmowym;
    c) pomieszczenia wyposażone są w szafki, dające gwarancje bezpieczeństwa dokumentacji i nośników danych;
    d) dokumentacja bieżąca i archiwalna przechowywana jest w obszarach przetwarzania danych osobowych w szafach zamykanych na zamki.
3. ADO stosuje następujące środki organizacyjne:
    a) opracowuje i wdraża Politykę;
    b) opracowuje i wdraża Politykę Bezpieczeństwa Informacji Systemów IT;

c) zapoznaje każdą osobę, przed przystąpieniem do pracy przy przetwarzaniu danych osobowych, z przepisami dotyczącymi ochrony danych osobowych;
d) regularnie szkoli osoby przetwarzające dane osobowe w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych;
e) zobowiązuje osoby przetwarzające dane osobowe do przestrzegania zasad ochrony danych osobowych;
f) kontroluje otwieranie i zamykanie pomieszczeń; pierwsza osoba rozpoczynająca pracę otwiera pomieszczenia, ostatnia – zamyka i uzbraja alarm;
g) kontroluje, aby w czasie pracy pomieszczenia nie pozostawały bez nadzoru, a w szczególności, aby w miejscu przetwarzania danych osobowych nie przebywały osoby nieupoważnione;
h) przyjmuje pisemne oświadczenie osoby upoważnionej do przetwarzania danych osobowych, że została zapoznana z przepisami dotyczącymi ochrony danych osobowych, w niniejszej Polityce, Polityce Bezpieczeństwa Informacji Systemów IT oraz że zobowiązuje się do ich przestrzegania;
i) nadzoruje przestrzeganie wszelkich wewnętrznych regulaminów i instrukcji dotyczących bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualnych zakresów zadań osób zatrudnionych przy przetwarzaniu danych osobowych, w tym dokumentów zawartych w niniejszej Polityce.

§ 8.

1. Wszystkie osoby zobowiązane są do przetwarzania danych osobowych zgodnie z obowiązującymi przepisami i zgodnie z ustaloną przez Administratora Danych niniejszą Polityką, Polityką Bezpieczeństwa Informacji Systemów IT, a także innymi dokumentami wewnętrznymi i procedurami związanymi z Przetwarzaniem danych osobowych w Spółce.
2. Wszystkie dane osobowe w Centro-chem sp. z o.o. sp.k. są przetwarzane z poszanowaniem zasad przetwarzania przewidzianych przez przepisy prawa:
    1) w każdym wypadku występuje chociaż jedna z przewidzianych przepisami prawa podstaw dla przetwarzania danych;
    2) dane są przetwarzane są rzetelnie i w sposób przejrzysty;
    3) dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
    4) dane osobowe są przetwarzane jedynie w takim zakresie, jaki jest niezbędny dla osiągnięcia celu przetwarzania danych;
    5) dane osobowe są prawidłowe i w razie potrzeby uaktualniane;
    6) czas przechowywania danych jest ograniczony do okresu ich przydatności do celów, do których zostały zebrane, a po tym okresie są one anonimizowane bądź usuwane;

7) wobec osoby, której dane dotyczą, wykonywany jest obowiązek informacyjny zgodnie z treścią art. 13 i 14 RODO.
8) dane są zabezpieczone przed naruszeniami zasad ich ochrony.

§ 9.

1. W przypadku stwierdzenia naruszenia ochrony danych osobowych Administrator dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.
2. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony Danych osobowych uważa się w szczególności:
   1) naruszenie bezpieczeństwa Systemów informatycznych, w których przetwarzane są dane osobowe, w razie ich przetwarzania w takich systemach;
   2) udostępnianie lub umożliwienie udostępniania danych osobom lub podmiotom do tego nieupoważnionym;
   3) zaniechanie, choćby nieumyślne, dopełnienia obowiązku zapewnienia danym osobowym ochrony;
   4) niedopełnienie obowiązku zachowania w tajemnicy Danych osobowych oraz sposobów ich zabezpieczenia;
   5) przetwarzanie Danych osobowych niezgodnie z założonym zakresem i celem ich zbierania;
   6) spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nieuprawnione kopiowanie Danych osobowych;
   7) naruszenie praw osób, których dane są przetwarzane.
3. W przypadku stwierdzenia okoliczności naruszenia zasad ochrony danych osobowych Użytkownik zobowiązany jest do podjęcia wszystkich niezbędnych kroków, mających na celu ograniczenie skutków naruszenia i do niezwłocznego powiadomienia Administratora Danych.
4. W każdej sytuacji, w której 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 nr 6** do niniejszej Polityki.
5. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator zawiadamia o incydencie także osobę, której dane dotyczą.
6. Administrator zapewnia zgłaszanie naruszeń ochrony danych osobowych Organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. W tym celu Administrator w szczególności zobowiązuje wszystkie osoby przetwarzające dane osobowe do niezwłocznego informowania o każdym dostrzeżonym naruszeniu ochrony danych osobowych.

7. W każdym wypadku Administrator bada zaistniałe naruszenie i wdraża stosowne organizacyjne i techniczne środki naprawcze.
8. ADO prowadzi rejestr zgłoszeń naruszeń.
9. Zgłoszenie naruszenia zawiera następujące informacje:
    1) charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
    2) imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
    3) możliwe konsekwencje naruszenia ochrony danych osobowych;
    4) 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.
10. ADO dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.
11. ADO może udzielić pełnomocnictwa innej osobie, również zatrudnionej w zakładzie pracy ADO, w zakresie przeprowadzenia procedury związanej z naruszeniem przetwarzania danych osobowych, pod warunkiem braku konfliktu interesu strony, w której doszło do naruszenia.

§ 10.

1. Do obowiązków Administratora Danych w zakresie zatrudniania, zakończenia lub zmiany warunków zatrudnienia pracowników lub współpracowników (osób podejmujących czynności na rzecz Administratora Danych na podstawie innych umów cywilnoprawnych) należy dopilnowanie, by:
    a) pracownicy byli odpowiednio przygotowani do wykonywania swoich obowiązków;
    b) każdy pracownik zobowiązał się do zachowania danych osobowych przetwarzanych w spółce w tajemnicy. „Oświadczenie i zobowiązanie osoby przetwarzającej dane osobowe do zachowania tajemnicy” stanowi element „Upoważnienia do przetwarzania danych osobowych”.
2. Administrator identyfikuje i weryfikuje podstawy prawne przetwarzania danych osobowych, a w szczególności:
    a) utrzymuje system zarządzania zgodami na przetwarzanie danych osobowych;
    b) inwentaryzuje i przygotowuje uzasadnienia przypadków, gdy dochodzi do przetwarzania danych osobowych na podstawie prawnie uzasadnionych interesów Administratora.

§ 11.

1. Administrator wywiązuje się z obowiązków informacyjnych względem osób, których dane dotyczą. W szczególności Administrator:

1) przekazuje osobom, których dane dotyczą wszelkie wymagane prawem informacje w czasie pozyskiwania danych osobowych, jak również w innych sytuacjach, gdy prawo wymaga przekazania dodatkowych informacji osobom, których dane dotyczą;
2) zapewnia dokumentację realizacji obowiązków, o których mowa w ust. 1 pkt. 1

2. Administrator zapewnia osobom, których dotyczą realizację praw przysługujących im na podstawie RODO. W szczególności Administrator dokłada starań, aby żądania osób, których dane dotyczą były realizowane w terminach wyznaczonych przez RODO oraz rzetelnie dokumentowane.
3. Administrator stosuje procedury działania w przypadku naruszenia ochrony danych osobowych, pozwalające na identyfikację i weryfikację naruszenia, a w razie potrzeby jego niezwłoczne zgłoszenie Urzędowi Ochrony Danych Osobowych oraz zawiadomienie osoby, której dane dotyczą.
4. Administrator stosuje metodykę zarządzania minimalizacją (privacy by default), która ustala zasady: zarządzania adekwatnością danych, reglamentacji i zarządzania dostępem do danych, zarządzania okresem przechowywania danych i weryfikacji dalszej przydatności.

§ 12.

1. Administrator ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania.
2. Administrator ustala przydatność oraz stosuje takie środki i podejście w szczególności jak:
   1) anonimizacji;
   2) szyfrowanie danych osobowych;
   3) inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
   4) środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.
3. Administrator zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:
   1) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;
   2) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;
   3) dostosowuje środki ochrony danych do ustalonego ryzyka;
   4) wdraża system zarządzania bezpieczeństwem informacji;
   5) zarządza incydentami naruszenia ochrony danych osobowych.

§ 13.

1. Każdy użytkownik zobowiązany jest do utrzymania właściwego poziomu bezpieczeństwa w zakresie swoich obowiązków i uprawnień.

2. Każdy użytkownik zobowiązany jest do przestrzegania polityki „czystego biurka", co oznacza, że:
    a) po zakończonej pracy wszystkie nośniki danych zawierające dane osobowe oraz dokumenty w formie tradycyjnej muszą być schowane do zamykanej szafy;
    b) każdy pracownik zobowiązany jest do przechowywania na biurku tylko tych dokumentów, które są pracownikowi niezbędne w danym momencie pracy do wykonania bieżących zadań;
    c) na biurku nie mogą znajdować się napoje w pojemnikach grożących rozlaniem płynu;
    d) w trakcie pracy, w razie wejścia osoby nieupoważnionej do pomieszczenia, w którym przetwarzane są dane osobowe, dokumenty muszą być ułożone w sposób uniemożliwiający ujawnienie danych osobowych;
    e) pracownik zobowiązany jest do niszczenia dokumentów niepotrzebnych w taki sposób, aby nie było możliwe odtworzenie zawartych w nich informacji, np. w niszczarce
    f) po zakończonej pracy na biurku mogą znajdować się jedynie telefon i przybory biurowe, takie jak: zszywacz, dziurkacz, długopis.
3. Każdy użytkownik zobowiązany jest do przestrzegania polityki „czystego ekranu", co oznacza, że w przypadku przebywania osoby nieupoważnionej w pomieszczeniu, w którym przetwarzane są dane osobowe, monitor musi być odwrócony w sposób uniemożliwiający odczytanie danych lub zabezpieczony wygaszaczem ekranu.
4. Każdy użytkownik zobowiązany jest do prowadzenia rozmów, w tym telefonicznych w taki sposób, aby informacje dotyczące danych osobowych nie zostały przekazane osobom nieupoważnionym.
5. Każdy użytkownik składa oświadczenie zgodnie ze wzorem określonym w **załączniku nr 7** do niniejszej Polityki, w którym:
    a) potwierdza zapoznanie się z Ustawą, Rozporządzeniem, niniejszą Polityką oraz Polityką Bezpieczeństwa Informacji Systemów IT;
    b) zobowiązuje się do zapewnienia ochrony przetwarzanych przez niego danych osobowych.
6. Osoby przetwarzające dane osobowe przy użyciu komputerów przenośnych zobowiązane są do przestrzegania dodatkowo następujących zasad:
    a) podczas transportu, przechowywania i użytkowania komputera przenośnego konieczne jest zachowanie szczególnej ostrożności;
    b) dane osobowe zlokalizowane na dyskach komputerów przenośnych podlegają ochronie kryptograficznej;

c) pozostawienie komputera przenośnego bez nadzoru w samochodzie, przechowalni, bagażu itp. jest niedozwolone;
d) Korzystający z komputera przenośnego zobowiązany jest do takiego użytkowania, aby uniemożliwić wgląd w wyświetlane na monitorze dane przez osoby nieupoważnione;
e) udostępnianie komputera przenośnego osobom nieupoważnionym jest zabronione.

7. Każdy użytkownik, również po zakończeniu współpracy z ADO, zobowiązany jest do ochrony wszelkich informacji dotyczących przetwarzanych danych osobowych, funkcjonowania systemów czy urządzeń służących do przetwarzania danych osobowych i sposobów zabezpieczania danych.
8. Przetwarzanie danych osobowych w sposób sprzeczny z niniejszą Polityką jest niedozwolone.
9. Użytkownicy, którzy nie zastosują się do zasad wynikających z niniejszej Polityki, Polityki Bezpieczeństwa Informacji Systemów IT, Ustawy i Rozporządzenia, mogą ponosić w uzasadnionych przypadkach odpowiedzialność wynikającą z przepisów prawa.
10. Przypadki nieuzasadnionego niezastosowania się przez pracownika do wskazanych w ust. 9 aktów potraktowane mogą zostać potraktowane jako ciężkie naruszenie podstawowych obowiązków pracowniczych.
11. Pracownicy zobowiązani są w szczególności do:
    a) ścisłego przestrzegania zakresu nadanego upoważnienia;
    b) przetwarzania i ochrony danych osobowych zgodnie z przepisami;
    c) zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
    d) zgłaszania incydentów związanych z naruszeniem bezpieczeństwa danych oraz niewłaściwym funkcjonowaniem systemu.
12. Pracownicy i Współpracownicy przetwarzający dane osobowe są zobowiązani w szczególności do:
    1) przetwarzania danych zgodnie z posiadanym upoważnieniem[3] oraz z należytą starannością;
    2) w przypadku zaobserwowania zdarzenia mogącego stanowić naruszenie ochrony danych osobowych, niezwłocznego informowania o nim bezpośredniego IOD;
    3) uczestnictwa w organizowanych szkoleniach z zakresu ochrony danych osobowych;
    4) zachowania w poufności danych osobowych oraz informacji na temat sposobu ich zabezpieczenia, zgodnie z podpisaną klauzulą poufności.

§ 14.

1. Administrator w celu zapewnienia ochrony danych osobowych może powołać Inspektora Ochrony Danych (IOD), zgodnie z wytycznymi określonymi w § 1 ust. 12 niniejszej Polityki. Powołanie odpowiednio na IOD stanowi **załącznik nr 9** do niniejszej Polityki.

[3] Załącznik nr 8

2. Inspektor Ochrony Danych realizując niniejszą Politykę, dokłada najwyższej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:
    1) przetwarzane zgodnie z prawem;
    2) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami;
    3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
    4) przechowywane nie dłużej niż jest to niezbędne do realizacji celów, w których zostały zebrane.
    5) Do obowiązków Inspektora Ochrony Danych (IOD) należą:
    1) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
    2) monitorowanie przestrzegania rozporządzenia RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
    3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
    4) współpraca z organem nadzorczym;
    5) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;
    6) pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia;
    7) prowadzenie rejestru czynności lub rejestru kategorii czynności.
3. IOD ma prawo do:
    1) wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych w całej organizacji;
    2) wstępu do pomieszczeń w których zlokalizowane są zbiory danych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z RODO, żądać złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego;

3) żądania okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli;
4) żądania udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych.

4. IOD wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.
5. Osoby, których dane dotyczą, mogą kontaktować się z IOD we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO pod adresem poczty elektronicznej:

iod@centro-chem.pl

§ 15.

1. Udostępnianie danych osobowych jest dopuszczalne tylko wtedy, gdy spełniony jest jeden z warunków, o którym mowa w art. 6 ust. 1 albo w art. 9 ust. 2 RODO. W przypadku powzięcia wątpliwości, czy dane osobowe powinny zostać udostępnione, należy skonsultować się z IOD.
2. Powierzenie przetwarzania danych osobowych podmiotowi trzeciemu następuje w oparciu o umowę powierzenia przetwarzania danych, po weryfikacji tego podmiotu w sposób określony w Polityce wyboru dostawcy przetwarzającego dane osobowe.
3. Wzór umowy, o której mowa w ust. 3, stanowi **załącznik nr 10** do niniejszej Polityki.
4. Wykaz podmiotów, którym powierzono przetwarzanie danych osobowych znajduje się w **załączniku nr 11** do niniejszej Polityki.
5. Dane osobowe przetwarzane przez ADO mogą być udostępnione podmiotowi, którego dane dotyczą lub innym podmiotom przez niego upoważnionym.
6. Ponadto dane osobowe mogą być udostępnione innym podmiotom jedynie w celu realizacji umowy zawartej pomiędzy ADO, a osobą, której dane dotyczą lub podmiotom upoważnionym ustawowo.

§ 16.

1. Administrator na bieżąco weryfikuje czy dane osobowe nie są przekazywane do państw trzecich (tj. poza Europejski Obszar Gospodarczy) lub do organizacji międzynarodowych.
2. W przypadku przekazywania danych osobowych do państw trzecich lub do organizacji międzynarodowych Administrator zapewnia zgodność przekazywania danych z RODO.
3. Administrator na bieżąco weryfikuje, czy zachodzą przypadki transgranicznego przetwarzania danych osobowych.

§ 17.

1. Obszar, w którym przetwarzane są Dane osobowe na terenie Centro-chem sp. z o.o. sp.k. są w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych znajdujących się w pomieszczeniach biurowych zlokalizowanych w Turce, Turka 141B, 20-258

Lublin. Wykaz pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe stanowi **Załącznik nr 12** do niniejszej Polityki.

2. Dodatkowo obszar, w którym przetwarzane są Dane osobowe, stanowią wszystkie komputery przenośne oraz inne nośniki danych znajdujące się poza obszarem wskazanym powyżej.
3. Administrator zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości Przetwarzanych danych.
4. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych, Środki obejmują:
    1) ograniczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe, jedynie do osób odpowiednio upoważnionych. Inne osoby mogą przebywać w pomieszczeniach wykorzystywanych do przetwarzania danych jedynie w towarzystwie osoby upoważnionej;
    2) zamykanie pomieszczeń tworzących obszar Przetwarzania danych osobowych na czas nieobecności pracowników, w sposób uniemożliwiający dostęp do nich osób trzecich;
    3) wykorzystanie zamykanych szafek i sejfów do zabezpieczenia dokumentów;
    4) wykorzystanie niszczarki do skutecznego usuwania dokumentów zawierających dane osobowe;
    5) ochronę sieci lokalnej przed działaniami inicjowanymi z zewnątrz przy użyciu sieci firewall;
    6) wykonywanie kopii awaryjnych danych na dyskach przenośnych zabezpieczonych przy pomocy haseł dostępu;
    7) ochronę sprzętu komputerowego wykorzystywanego u administratora przed złośliwym oprogramowaniem;
    8) zabezpieczenie dostępu do urządzeń znajdujących się w siedzibie spółki przy pomocy haseł dostępu;
    9) wykorzystanie szyfrowania danych przy ich transmisji.
5. Administrator wdraża odpowiednie środki, aby komunikacja z Podmiotem danych odbywała się w zwięzłej, przejrzystej i łatwo dostępnej formie.
6. Przyjmowanie i obsługa żądań Podmiotów danych odbywa się na zasadach określonych w niniejszej Polityce obsługi żądań Podmiotów danych dotyczących realizacji praw związanych z przetwarzaniem danych.

§ 18.

1. Administrator zapewnia stałe monitorowanie zgodności działania Spółki z zasadami ochrony danych osobowych.

2. Do podejmowania czynności związanych z zapewnieniem zgodności zobowiązany jest IOD. Każdy pracownik i współpracownik Spółki zobowiązany jest wspierać IOD w wykonywaniu jego zadań, w szczególności udzielać niezbędnych informacji i wyjaśnień.

§ 19.

Bezpieczeństwo informacji i ochrona danych osobowych w ramach pracy zdalnej

1. Poniższa procedura opisuje sposób zapewnienia bezpieczeństwa informacji i ochrona danych osobowych w ramach pracy zdalnej.
2. Przyjęto, że Pracownik zobowiązuje się do zabezpieczania dostępu do sprzętu służbowego oraz posiadanych danych i informacji (w tym także znajdujących się na nośnikach papierowych) przed osobami postronnymi, w tym wspólnie z nim zamieszkującymi.
3. Wykonywanie pracy w formie zdalnej nie zwalnia pracownika z obowiązku przestrzegania postanowień Polityce Ochrony Danych Osobowych Spółki wraz z dokumentami powiązanymi, w tym Polityka Bezpieczeństwa Informacji Systemów IT. Pracownik zobowiązany jest do złożenia oświadczenia w zakresie stosowania w/w regulacji.
4. Pracownik posługuje się przekazanymi przez pracodawcę danymi dostępowymi (w tym loginami, hasłami) do systemów informatycznych i poczty elektronicznej i zapewnia ochronę tych danych, a także przetwarzanych w ramach takiego dostępu danych osobowych i informacji, w szczególności przed dostępem osób nieuprawnionych, ich zniszczeniem i utratą.
5. Pracownik zgłasza wszelkie incydenty bezpieczeństwa i ochrony danych osobowych, a także podejrzenia ich wystąpienia oraz wszelkie nieprawidłowości w zakresie ochrony danych osobowych, do osób odpowiedzialnych za ochronę danych osobowych i bezpieczeństwo informacji w zakładzie pracy.

§ 20.

1. Urządzenia i oprogramowanie przekazane przez Centro-chem sp. z o.o. sp.k do pracy zdalnej służą do wykonywania obowiązków służbowych.
2. Pracownik obowiązany jest w szczególności do:
    1) nie instalowania dodatkowych aplikacji i oprogramowania niezgodnych z procedurą bezpieczeństwa;
    2) upewnienia się, że wszystkie urządzenia z jakich korzystasz mają niezbędne aktualizacje systemu operacyjnego (IOS lub Android), oprogramowania oraz systemu anty-wirusowego;
    3) wydzielenia odpowiedniej przestrzeni, tak aby ewentualne osoby postronne, nie miały dostępu do dokumentów, nad którymi pracownik pracuje. Odchodząc od stanowiska pracy każdorazowo należy blokować urządzenie, na którym pracownik pracuje;
    4) zabezpieczenia komputera poprzez używanie silnych haseł dostępu oraz wielopoziomowe uwierzytelnianie, co pozwoli to na ograniczenia dostępu do

urządzenia, a jednocześnie na ograniczenia ryzyka utraty danych w przypadku kradzieży lub zgubienia urządzenia;

§ 20.

1. W ramach pracy zdalnej Administrator może dokonywać kontroli w zakresie bezpieczeństwa i ochrony informacji, w tym procedur ochrony danych osobowych.
2. Kontrola obejmuje w szczególności:
    1) kontrolę sposobu przestrzegania przez pracownika obowiązujących zasad ochrony danych osobowych przyjętych u pracodawcy, w tym w zakresie stosowania zabezpieczeń adresowanych przez pracowników;
    2) potwierdzenie uczestnictwa pracownika w szkoleniach z zakresu ochrony danych osobowych;
    3) potwierdzenie stosowania obowiązujących u pracodawcy procedur ochrony danych osobowych;
    4) kontrolę narzędzi i systemów, za pośrednictwem których pracownik uzyskuje dostęp do danych osobowych pracodawcy.
3. Przeprowadzenie kontroli przestrzegania wymogów w zakresie bezpieczeństwa i ochrony informacji, w tym procedur ochrony danych osobowy polega na sprawdzeniu w szczególności:
    1) czy pracownik komunikuje się z pracodawcą i innymi pracownikami przy użyciu służbowej poczty elektronicznej;
    2) czy dane osobowe nie zostały udostępnione osobom nieuprawnionym;
    3) czy pracownik korzysta z udostępnionych przez pracodawcę systemów informatycznych, w których przetwarzane są dane osobowe;
    4) czy pomieszczenie, w którym przetwarzane są dane osobowe zapewnia ich zabezpieczenie przed nieuprawnionym dostępem osób trzecich, w szczególności, czy ustawienie monitora zapewnia poufność danych osobowych;
    5) czy pracownik zna ścieżki i terminy zgłaszania incydentów ochrony danych i podejrzeń takich incydentów;
    6) czy pracownik zna tożsamość i dane kontaktowe osób odpowiedzialnych za bezpieczeństwo informacji i ochronę danych osobowych;
    7) czy pracownik stosuje środki organizacyjne i techniczne niezbędne do ochrony danych osobowych, przyjęte w organizacji, np. szyfrowanie, pseudonimizację;
    8) czy w otoczeniu pracownika znajduje się niezabezpieczona dokumentacja zawierająca dane osobowe;
    9) czy pracownik systematycznie usuwa zbędne dane osobowe i niszczy niepotrzebną, roboczą dokumentację.

4. Kontrola należytego przestrzegania zasad w zakresie bezpieczeństwa i ochrony informacji, w tym procedur ochrony danych osobowych odbywa przy wykorzystaniu środków komunikacji elektronicznej, a także może odbywać się w miejscu wykonywania pracy zdalnej.
5. Kontrola, o której mowa w ust. 3, może być wykonywana przy wykorzystaniu środków komunikacji elektronicznej, w tym za pomocą lub przy użyciu:
    1) służbowego telefonu udostępnionemu pracownikowi;
    2) służbowej poczty elektronicznej;
    3) stosowanych w zakładzie pracy komunikatorów lub chatu wewnętrznego

– w godzinach pracy obowiązujących pracownika, bez wcześniejszego uprzedzenia przez pracodawcę.

6. W ramach kontroli przeprowadzanej przy wykorzystaniu środków komunikacji elektronicznej, pracodawca może żądać spotkania online z pracownikiem, przebiegającego ze wzajemnym ujawnieniem wizerunków, a także otoczenia, w którym pracownik wykonuje pracę zdalną. Pracownik zapewnia, że w otoczeniu nie będą znajdować się członkowie jego rodziny lub inne osoby przebywające w jego miejscu zamieszkania.
7. Szczegółowe zasady organizacji i kontroli ochrony danych osobowych w zakresie pracy zdalnej określa Procedura ochrony danych osobowych w zakresie pracy zdalnej w spółce Centro-Chem Sp. z o.o. Sp.k.

§ 21.

Korzystanie z plików cookies.

1. Poniższa procedura opisuje sposób korzystania przez Użytkowania z Serwisu, przez który należy przez to rozumieć serwis internetowy prowadzony przez Administratora pod adresem **https://www.centro-chem.pl.**

   Użytkownikiem jest każda osobę fizyczną odwiedzającą Serwis lub korzystająca z jednej albo kilku usług czy funkcjonalności.
2. W związku z korzystaniem przez Użytkownika z Serwisu Administrator zbiera dane w zakresie niezbędnym do świadczenia poszczególnych oferowanych usług.
3. Dane osobowe, które Użytkownik poda w Serwisie lub które Administrator zbierze na temat Użytkowania są przetwarzane zgodnie z Rozporządzeniem, Ustawą i innymi aktami prawnymi, które regulują ochronę danych osobowych na szczeblu krajowym i europejskim.
4. Administrator stosuje wymagane aktualnymi przepisami o ochronie danych osobowych środki techniczne zapobiegające pozyskiwaniu i modyfikowaniu przez osoby nieuprawnione danych osobowych przesyłanych drogą elektroniczną, czyli w ramach Serwisu.
5. Dane osobowe wszystkich osób korzystających z Serwisu przetwarzane są przez Administratora w celu:

1) świadczenia usług drogą elektroniczną w zakresie udostępniania Użytkownikom treści gromadzonych w Serwisie – wówczas podstawą prawną przetwarzania jest niezbędność przetwarzania do wykonania umowy (art. 6 ust. 1 lit. b RODO);
2) ustalenia i dochodzenia roszczeń lub obrony przed roszczeniami – podstawą prawną przetwarzania jest prawnie uzasadniony interes Administratora (art. 6 ust. 1 lit. f RODO), polegający na ochronie jego praw.

6. Administrator zapewnia możliwość skontaktowania się z nim przy wykorzystaniu elektronicznego formularza kontaktowego. Skorzystanie z formularza wymaga podania Danych osobowych niezbędnych do nawiązania kontaktu z Użytkownikiem i udzielenia odpowiedzi na zapytanie.
7. Dane osobowe są przetwarzane w celu identyfikacji nadawcy oraz obsługi jego zapytania przesłanego przez udostępniony formularz – podstawą prawną przetwarzania jest niezbędność przetwarzania do wykonania umowy o świadczenie usługi (art. 6 ust. 1 lit. b RODO); w zakresie danych podanych fakultatywnie podstawą prawną przetwarzania jest zgoda (art. 6 ust. 1 lit. a RODO).
8. Dane osobowe Użytkownika mogą być również wykorzystywane przez Administratora, aby kierować do niego treści marketingowe różnymi kanałami, tj. za pośrednictwem poczty e-mail, drogą MMS/SMS. Takie działania są podejmowane przez Administratora wyłącznie w przypadku, gdy Użytkownik wyraził na nie zgodę, którą może wycofać w dowolnym momencie.
9. Szczegółowe zasady przetwarzania danych osobowych Użytkowników oraz czas ich przetwarzania określa Polityka prywatności dostępna na stronie: https://centro-chem.pl/polityka-prywatnosci/.

§ 21.

Przekazywanie danych poza Europejskim Obszarem Gospodarczym

1. Administrator może, tylko wtedy gdy jest to konieczne, przekazać dane osobowe poza Europejski Obszar Gospodarczy, zwanej dalej „EOG”, i z zapewnieniem odpowiedniego stopnia ochrony, przede wszystkim poprzez:
   1) współpracę z podmiotami przetwarzającymi dane osobowe w państwach, w odniesieniu do których została wydana stosowna decyzja Komisji Europejskiej;
   2) stosowanie standardowych klauzul umownych wydanych przez Komisję Europejską;
   3) stosowanie wiążących reguł korporacyjnych zatwierdzonych przez właściwy organ nadzorczy;
   4) w razie przekazywania danych do USA – współpracę z podmiotami uczestniczącymi w programie Tarcza Prywatności (ang. Privacy Shield) zatwierdzonym decyzją Komisji Europejskiej.

2. Administrator zawsze informuje o zamiarze przekazania danych osobowych poza EOG na etapie ich zbierania

§ 22.

Procedura prywatności dla kandydatów do pracy w Centro-chem sp. z o.o. sp.k

1. Poniższa procedura zawiera informacje na temat danych osobowych, które zbiera Centro-chem sp. z o.o. sp.k – Administrator - w ramach prowadzonych rekrutacji. Centro-chem sp. z o.o. sp.k. w odniesieniu do danych osobowych kandydatów do pracy w Spółce bez względu na podstawę prawną zatrudnienia.
2. W celu prowadzenia działalności, Spółka zbiera i wykorzystuje informacje identyfikujące osoby fizyczne – dane osobowe - w tym informacje o naszych przyszłych, obecnych i byłych pracownikach oraz osobach współpracujących w ramach umów prawa cywilnego.
3. Niniejsza polityka dotyczy wszelkich form wykorzystywania przez nas danych osobowych („przetwarzanie") w odniesieniu do danych osobowych kandydatów do pracy w Spółce („Kandydaci") bez względu na podstawę prawną zatrudnienia. Klauzula informacyjna o przetwarzaniu danych osobowych dla kandydatów do pracy w Centro-chem sp. z o.o. sp.k stanowi **załącznik nr 13** do niniejszej Polityki.
4. Centro-chem sp. z o.o. sp.k w celach rekrutacyjnych do pracy zbiera podstawowe dane wskazane w art. 22^1 § 1 Kodeksu pracy[4], takie jak imię (imiona) i nazwisko, data urodzenia, wykształcenie, przebieg dotychczasowego zatrudnienia, a także inne dane osobowe, gdy jest to niezbędne do wypełniania obowiązku pracodawcy nałożonego przepisem prawa. Podanie tych danych przez Kandydatów jest wymogiem ustawowym (w przypadku Kandydatów zatrudnianych w oparciu o umowę o pracę). Konsekwencją niepodania danych jest niemożność nawiązania zatrudnienia oraz brak możliwości prowadzenia procesu rekrutacyjnego.
5. Przetwarzane przez Centro-chem sp. z o.o. sp.k dane osobowe mogą również obejmować specjalne, szczególnie wrażliwe kategorie danych, takie jak informacje dotyczące stopnia niepełnosprawności. Takie kategorie danych będą szczególnie chronione przez Spółkę. W szczególności takie dane nie będą udostępniane żadnym niepowołanym osobom.
6. Centro-chem sp. z o.o. sp.k może również zbierać Kandydatów dane osobowe od podmiotów świadczących usługi rekrutacyjne lub agencji zatrudnienia, agencji świadczących usługi outplacement, biur karier, a także portali internetowych (w tym dedykowanych portali społecznościowych) umożliwiających kontakt pomiędzy pracodawcami a kandydatami do pracy, jeżeli istnieje ku temu odpowiednia podstawa prawna. Pozyskując takie informacje, Spółka nie będzie nadmiernie ingerowała w prywatność Kandydata, ograniczy się jedynie do danych osobowych z obszaru zawodowego oraz będzie przetwarzała takie dane jedynie w celach związanych z prowadzeniem rekrutacji.

[4] Ustawa z dnia

7. Centro-chem sp. z o.o. sp.k przetwarza dane osobowe tylko wtedy, gdy:
    1) przetwarzanie jest niezbędne do wypełniania zobowiązań umownych wobec Kandydatów lub zgodnie z Kandydata żądaniem jest niezbędne do podjęcia konkretnych czynności przed zawarciem umowy, w tym do przeprowadzenia procesu rekrutacyjnego;
    2) przetwarzanie jest konieczne w celu wywiązania się z naszych obowiązków prawnych lub wprost nakazuje nam to przepis prawa (np. art. 22^1 Kodeksu pracy);
    3) przetwarzanie jest niezbędne dla realizacji uzasadnionych interesów Spółki lub strony trzeciej i nie wpływa nadmiernie na Kandydata interesy ani podstawowe prawa i wolności. Należy pamiętać, że podczas przetwarzania danych osobowych na tej podstawie Spółka stara się zachować równowagę między uzasadnionym interesem Spółki a Kandydata prywatnością. Takimi „uzasadnionymi interesami" są:
        a) spełnianie celów Spółki dotyczących odpowiedzialności korporacyjnej i społecznej;
        b) ustalanie lub dochodzenie przez Spółkę roszczeń cywilnoprawnych w ramach prowadzonej działalności, a także obrona przed takimi roszczeniami;
        c) środki powzięte w celu utrzymania działań operacyjnych (np. planowanie zatrudnienia w Spółce, planowanie budżetu, planowanie przestrzeni itp.);
    4) w niektórych przypadkach, gdy Spółka uzyskała od Kandydata wcześniejszą zgodę.
8. Szczególne kategorie danych osobowych mogą być przetwarzane przez Spółkę jedynie w szczególnych przypadkach, tj. gdy przetwarzanie jest niezbędne do realizacji zobowiązań Spółki wynikających z zatrudnienia, zabezpieczenia społecznego lub ochrony socjalnej - dotyczy to danych osobowych obejmujących stopień niepełnosprawności i związane z nim szczególne uprawnienia.

§ 23.

1. Jeżeli Spółka przetwarza dane osobowe Kandydata na podstawie zgody, może być ona odwołana w każdej chwili w sposób równie łatwy, jak została udzielona. Niewyrażenie zgody na przetwarzanie danych, do których podania nie są Kandydaci zobowiązani, nie będzie skutkowało odmową nawiązania stosunku pracy z Kandydatem, a jej odwołanie nie spowoduje negatywnych konsekwencji dla Kandydata.
2. Spółka przetwarza dane osobowe Kandydata w określonym celu i przetwarza tylko te dane osobowe, które są konieczne dla jego osiągnięcia. W szczególności Spółka przetwarza dane osobowe Kandydatów w celu:
    1) podejmowania działań rekrutacyjnych;
    2) przygotowania umów dotyczących zatrudnienia Kandydatów;
    3) zarządzania dokumentacją pracowniczą;

4) przestrzegania wszelkich obowiązków prawnych nałożonych na Spółkę w stosunku do Kandydatów.

3. Spółka może przekazywać dane osobowe odbiorcom oraz innym stronom trzecim, aby realizować cele wymienione w ust. 2 w zakresie, w jakim są one dla nich niezbędne do wykonania zadań zleconych przez Spółkę, jeżeli wymaga od Spółki przepis prawa. Za odbiorców lub inne strony trzecie mogą być uznane:
    1) podmioty przetwarzające dane osobowe na zlecenie Spółki, takie jak:
        a) dostawcy do Spółki systemów informatycznych oraz usług hostingowych,
        b) podmioty świadczące usługi archiwizacji dokumentów.

W/w podmioty nie decydują samodzielnie o tym, w jaki sposób przetwarzać dane osobowe Kandydatów. Przetwarzanie przez nie danych osobowych ma miejsce tylko w zakresie, w jakim jest to niezbędne dla prowadzenia działalności przez Spółkę. Spółka ma kontrolę nad działaniem takich podmiotów za pomocą odpowiednich zapisów umownych chroniących prywatność Kandydatów;

2) podmioty takie, jak:
    a) agencje rekrutacyjne lub agencje pracy tymczasowej,
    b) doradcy prawni lub podatkowi,
    c) dostawcy usług kurierskich lub pocztowych.

Tego typu podmioty są samodzielnymi administratorami danych. Oznacza to, że Spółka nie ma wpływu na to, w jaki sposób oraz w jakim zakresie przetwarzają one dane osobowe Kandydatów. Spółka nie jest odpowiedzialna za zgodność działalności takich podmiotów z przepisami;

3) wszelkie krajowe organy administracji publicznej, organy innych państw członkowskich UE (np. organy powołane do ochrony danych osobowych w innych państwach członkowskich) lub sądy, jeżeli jest to wymagane przez obowiązujące prawo krajowe lub unijne albo na ich żądanie.

4. Dane osobowe przekazywane w ramach Spółki mogą być również przetwarzane w kraju znajdującym się poza EOG, który obejmuje państwa członkowskie UE, Islandię, Liechtenstein i Norwegię. Kraje spoza EOG mogą nie oferować takiego samego poziomu ochrony danych osobowych jak kraje EOG.
5. Jeżeli dane osobowe Kandydatów zostaną w przyszłości przekazane poza EOG innym podmiotom, Spółka wprowadzi odpowiednie zabezpieczenia w celu zapewnienia, że takie przekazywanie jest przeprowadzane zgodnie z obowiązującymi zasadami ochrony danych. Aby zapewnić odpowiedni poziom ochrony danych osobowych, Spółka może przykładowo skorzystać z umowy o powierzenie przetwarzania danych z odbiorcą będącym osobą trzecią na podstawie standardowych klauzul ochrony danych zatwierdzonych przez Komisję Europejską lub zapewnić, że przeniesienie nastąpi na teren jurysdykcji, która jest przedmiotem decyzji Komisji Europejskiej w sprawie odpowiedniej ochrony danych osobowych.

6. Spółka przechowuje dane osobowe tylko tak długo, jak to konieczne, aby osiągnąć cel, w którym zostały one zgromadzone lub aby było to zgodne z wymogami prawnymi.
7. Dane osobowe Kandydatów są przetwarzane przez cały czas trwania procesu rekrutacji. Po upływie tego czasu dane osobowe Kandydatów w zakresie informacji o przeprowadzonej rekrutacji będą przetwarzane przez okresy przedawnienia roszczeń cywilnoprawnych w celu umożliwienia Spółce obrony przed ewentualnymi roszczeniami lub dochodzenia takich roszczeń, jeżeli zaistnieje ryzyko wysunięcia takich roszczeń przez lub w stosunku do Spółki; zgodnie z polskim prawem co do zasady jest to okres nie dłuższy niż 3 lata od momentu zakończenia procesu rekrutacyjnego.
8. Jeżeli Kandydat pragnie, aby dotyczące dane osobowe Kandydata zostały usunięte z baz danych Spółki, istnieje możliwość złożenia wniosku zgodnie z informacjami zawartymi w ust. 10.
9. Kandydat ma prawo dostępu do swoich danych osobowych przetwarzanych przez Spółkę. Jeśli Kandyda uważa, że jakiekolwiek informacje dotyczące osoby Kandydata są nieprawidłowe lub niekompletne, ma również prawo wnieść o ich sprostowanie w sposób określony w ust. 10. poniżej.
10. Kandydat ma również prawo do:
    1) wycofania zgody w przypadku, gdy Spółka uzyskała taką zgodę na przetwarzanie danych osobowych (przy zastrzeżeniu, że wycofanie to nie naruszy zgodności z prawem przetwarzania danych dokonanego przed wycofaniem);
    2) żądania usunięcia danych osobowych;
    3) żądania ograniczenia przetwarzania danych osobowych;
    4) sprzeciwienia się – z przyczyn związanych z szczególną sytuacją – wobec przetwarzania danych osobowych (w tym profilowania), jeżeli takie przetwarzanie dokonywane jest w celu realizacji interesu publicznego lub uzasadnionych interesów Spółki lub strony trzeciej;
    5) przeniesienia danych, tj. otrzymania danych osobowych przekazanych Spółce w ustrukturyzowanym, powszechnie używanym i możliwym do odczytu maszynowego formacie oraz do żądania przesłania takich danych osobowych do innego administratora danych osobowych, bez utrudnień ze strony Spółki i z zastrzeżeniem własnych zobowiązań dotyczących poufności.
11. Spółka będzie weryfikować prośby Kandydatów, żądania lub sprzeciwy zgodnie z obowiązującymi przepisami o ochronie danych osobowych. Prawa te nie mają charakteru bezwzględnego; przepisy przewidują wyjątki od ich stosowania.
12. Z powyższych uprawnień Kandydaci mogą skorzystać, kontaktując się drogą korespondencyjną ze Spółką Centro-Chem spółka z ograniczoną odpowiedzialnością spółka komandytowa, Turka 141B, 20-258 Lublin, lub wysyłając wiadomość e-mail na adres iod@centro-chem.pl.

§ 24.
Ocena Skutków (Analiza Ryzyka)

1. Ocena skutków jest formalną, określoną w art. 35 RODO procedurą przeprowadzenia analizy ryzyka za wykonanie której odpowiada ADO. Jeżeli ADO nie jest zobowiązany do przeprowadzenia analizy oceny skutków, może mimo to stosować poniższą procedurę do przeprowadzenia analizy ryzyka na potrzeby wykazania rozliczalności spełnienia wymagań RODO. W przypadku powołania Inspektora Ochrony Danych Osobowych – ocena skutków musi być wykonana z jego współudziałem.
2. W ramach przeprowadzenia oceny skutków (analizy ryzyka) Administrator zobowiązany jest do spełnienia obowiązków prawnych wobec danych w zbiorach. W szczególności należy zapewnić, że:
    1) dane te są legalnie przetwarzane (na podstawie art. 6, 9 RODO);
    2) dane te są adekwatne w stosunku do celów przetwarzania;,
    3) dane te są przetwarzane przez określony czas (retencja danych);,
    4) wobec tych osób wykonano tzw. obowiązek informacyjny (art. 12, 13 i 14 RODO) wraz ze wskazaniem ich praw (np. prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, odwołania zgody);
    5) opracowano klauzule informacyjne dla powyższych osób;
    6) istnieją umowy powierzenia z podmiotami przetwarzającymi (art. 28 RODO);

§ 25.
Analiza Ryzyka

1. Niniejsza procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych. Przyjęto, że analiza ryzyka przeprowadzana jest dla zbioru lub grupy zbiorów (kategorii osób) lub dla procesów przetwarzania (np. dla zbioru pracowników, zbioru klientów, dla procesu wysyłania informacji handlowej z bazy marketingowej banku).
2. Ilekroć w dalszej części niniejszej procedurze, o której mowa w ust. 1, jest mowa bez bliższego określenia o:
    1) **Aktywach** – należy przez to rozumieć środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych;

2) **Naruszeniu (Incydencie) ochrony danych osobowych** – należy przez to rozumieć naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
3) **Zagrożeniu** – należy przez to rozumieć potencjalne naruszenie (potencjalny incydent);
4) **Skutkach** – należy przez to rozumieć rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia);
5) **Ryzyku** – należy przez to rozumieć prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów.

3. Przy wyznaczaniu zagrożeń
   1) Administrator jest odpowiedzialny za określenie listy zagrożeń naruszenia poufności, dostępności i integralności, które mogą wystąpić w przetwarzaniu danych w zbiorze, dla kategorii osób lub w procesie przetwarzania,
   2) Zagrożenia powinny być identyfikowane w odniesieniu do uprzednio zidentyfikowanych aktywów.
4. Wyliczenie ryzyka dla zagrożeń obejmuje:
   1) Administrator określa Prawdopodobieństwo (P) wystąpienia poszczególnych zagrożeń w zbiorze (dla kategorii osób) lub w procesie przetwarzania, gdzie ustaloną skalę prawdopodobieństwa prezentuje Tabela A,
   2) Administrator określa Skutki (S) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne, gdzie ustaloną skalę Skutków prezentuje Tabela B,
   3) Administrator wylicza Ryzyka (R) dla wszystkich zagrożeń i ich skutków w/g formuły:

R=PxS

Tabela A **Prawdopodobieństwo wystąpienia zagrożenia (P)**	**Skala (Waga)**
zagrożenie niskie	1
zagrożenie średnie	2
zagrożenie wysokie	3

Tabela B **Skutki wystąpienia zagrożenia**	**Skala (Waga)**
małe (do 10.000 PLN, incydent prasowy lokalny)	1
średnie (10.000 - 100.000 PLN, incydent prasowy ogólnopolski)	2
duże (od 100.000 PLN, naruszenie prawa)	3

5. Porównanie wyliczonych ryzyk ze skalą i określenie dalszego postępowania z ryzykiem obejmuje:
    1) Administrator porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem;
    2) ustaloną skalę Ryzyka prezentuje Tabela C.

Tabela C Poziom ryzyka	**Wartość [R = P x S]**
ryzyko pomijalne i akceptowalne (akceptujemy)	1 - 2
ryzyko jest opcjonalne (akceptujemy albo obniżamy)	3 - 6
ryzyko jest nieakceptowalne (musimy obniżyć)	9

6. Reakcja na wartość ryzyka obejmuje:
    1) Akceptacja ryzyka - zabezpieczenia są właściwe - brak potrzeby stosowania dodatkowych zabezpieczeń;
    2) Działania obniżające ryzyko, które może zastosować Administrator:
        a) **Przeniesienie** – przerzucenie ryzyka (outsourcing, ubezpieczenie),
        b) **Unikanie** – eliminacja działań powodujących ryzyko, (np. zakaz wynoszenia komputerów przenośnych poza obszar organizacji),
        c) **Redukcja** – zastosowanie zabezpieczeń w celu obniżenia ryzyka (np. szyfrowanie pendrivów z danymi wynoszonych poza firmę);
    3) Analizę ryzyka przeprowadza się w ustalonym szablonie (dokumenty wewnętrzne Organizacji).
7. Ponowna analiza ryzyka przeprowadzana jest cyklicznie lub po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów/kategorii osób, realizacja nowych procesów przetwarzania, zmiany prawne).
8. Zarządzanie ryzykiem obejmuje także Plan postępowania z ryzykiem poprzez:
    1) wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne, określając Plan postępowania z ryzykiem (dokumenty wewnętrzne Organizacji);
    2) Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń**.**

§ 26.

Okres przetwarzania danych osobowych

1. Okres przetwarzania danych przez Administratora zależy od rodzaju świadczonej usługi i celu przetwarzania. Okres przetwarzania danych może także wynikać z przepisów, gdy stanowią one podstawę przetwarzania. W przypadku przetwarzania danych na podstawie uzasadnionego interesu Administratora, dane przetwarzane są przez okres umożliwiający realizację tego

interesu lub do zgłoszenia skutecznego sprzeciwu względem przetwarzania danych. Jeśli przetwarzanie odbywa się na podstawie zgody, dane przetwarzane są do jej wycofania. Gdy podstawę przetwarzania stanowi niezbędność do zawarcia i wykonania umowy, dane są przetwarzane do momentu jej rozwiązania.

2. Okres przetwarzania danych może być przedłużony w przypadku, gdy przetwarzanie jest niezbędne do ustalenia lub dochodzenia roszczeń lub obrony przed roszczeniami, a po tym okresie – jedynie w przypadku i w zakresie, w jakim będą wymagać tego przepisy prawa. Po upływie okresu przetwarzania dane są nieodwracalnie usuwane lub anonimizowane.

Rozdział III

Postanowienia końcowe

§ 27.

1. Za niedopełnienie obowiązków wynikających z niniejszego dokumentu pracownik ponosi odpowiedzialność na podstawie Kodeksu pracy, Przepisów o ochronie danych osobowych oraz Kodeksu karnego w odniesieniu do danych osobowych objętych tajemnicą zawodową.
2. Procedury nadawania uprawnień, metody i środki uwierzytelnienia oraz procedury tworzenia kopii zapasowych reguluje Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
3. Aktualizacji niniejszej Polityki dokonuje Administrator, który wszelkie propozycje zmian przedstawia podmiotowi odpowiedzialnemu za jej wdrożenie.
4. Niniejsza Polityka wchodzi w życie z dniem podpisania Uchwały Zarządu.
5. Niniejsza Polityka może podlegać dalszym zmianom. Jeżeli będzie to wymagane prawem, wszelkie informacje dotyczące przyszłych zmian lub uzupełnień w przetwarzaniu danych osobowych opisanym w niniejszej Polityce zostaną przekazane za pośrednictwem odpowiedniej formy komunikacji zazwyczaj używanej w Spółce.
6. Integralną część niniejszej Polityki bezpieczeństwa stanowią Załączniki.

§ 28.

Wykaz załączników

1. *Załącznik nr 1 –Klauzula zgody na przetwarzanie danych osobowych (zwykłych).*
2. *Załącznik nr 2 – Klauzula zgody na przetwarzanie danych szczególnych kategorii.*
3. *Załącznik nr 2a – Ogólna klauzula informacyjna.*
4. *Załącznik nr 3 – Ewidencja osób upoważnionych do przetwarzania danych osobowych.*
5. *Załącznik nr 4 – Rejestr Czynności Przetwarzania Danych Osobowych.*
6. *Załącznik nr 5 – Rejestr Kategorii Czynności Przetwarzania.*
7. *Załącznik nr 6 – Zgłoszenie naruszenia ochrony Danych Osobowych.*

8. *Załącznik nr 7 – Oświadczenie.*
9. *Załącznik nr 8 – Upoważnienie do przetwarzania Danych Osobowych.*
10. *Załącznik nr 9 – Wyznaczenie Inspektora Ochrony Danych.*
11. *Załącznik nr 10 – Umowa powierzenia przetwarzania Danych Osobowych.*
12. *Załącznik nr 11 – Wykaz podmiotów, którym powierzono przetwarzanie danych osobowych (znajduje się w oddzielnym pliku w formacie .xlsx)*
13. *Załącznik nr 12 – Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.*
14. *Załącznik nr 13 – Klauzula informacyjna o przetwarzaniu danych osobowych dla kandydatów do pracy w Centro-chem sp. z o.o. sp.k.*
15. *Załącznik nr 14 – Polityka Bezpieczeństwa Informacji Systemów IT.*

Załącznik nr 1
do Polityka Ochrony Danych Osobowych w spółce Centro-chem sp. z o.o. sp.k.

Przetwarzanie danych „zwykłych”

Czy zgadzasz się na przetwarzanie Twoich danych osobowych zamieszczonych w ..... przez nas: Centro-chem sp. z o.o. sp.k., z siedzibą w Turce, w celu……. (*określić cel*)

□ TAK □ NIE

.....

podpis osoby wyrażającej zgodę

Informacja o prawie do cofnięcia zgody

W każdej chwili masz prawo cofnąć zgodę na przetwarzanie Twoich danych osobowych. Cofnięcie zgody nie będzie wpływać na zgodność z prawem przetwarzania, którego dokonano na podstawie Twojej zgody przed jej wycofaniem.

Załącznik nr 2
do Polityka Ochrony Danych Osobowych w spółce Centro-chem sp. z o.o. sp.k.

Przetwarzanie danych szczególnych kategorii

Czy wyrażasz zgodę na przetwarzanie przez: Spółkę Centro-chem sp. z o.o. sp.k., z siedzibą w Turce, w celu [*usprawiedliwienia swojej nieobecności* / *uzyskania spłaty długu*, w tym *danych o stanie zdrowia Twoim i Twoich bliskich* / *inne*]

Twoich danych osobowych, które przekazałaś nam w *rozmowie* / *korespondencji emailowej* / *inne*?

Ponieważ dane szczególnych kategorii w tym *dotyczące zdrowia* / *inne* chronione są szczególnie, musimy prosić Cię o wyrażenie wyraźnej zgody na ich przetwarzanie.

Prosimy, wyraźnie potwierdź, że zgadzasz się, abyśmy przetwarzali podane przez Ciebie dane, o których mowa wyżej

☐ NIE

☐ TAK, zgadzam się na to, abyście przetwarzali podane przeze mnie dane, o których mowa wyżej, w tym dane szczególnych kategorii, w celu powyżej wskazanym*

** Dane szczególnych kategorii to dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne wykorzystywane do identyfikacji, dane dotyczące zdrowia, seksualności lub orientacji seksualnej*

(*Jeżeli organizacja zbiera kilka zgód dotyczących różnych celów przetwarzania, zgody te muszą zostać wyrażone osobno. Niedozwolone jest zbiorcze zbieranie zgód*)

Informacja o prawie cofnięcia zgody

W każdej chwili przysługuje Ci prawo do wycofania zgody na przetwarzanie Twoich danych osobowych. Cofnięcie zgody nie będzie wpływać na zgodność z prawem przetwarzania, którego dokonano na podstawie Twojej zgody przed jej wycofaniem.

Obowiązek informacyjny

W związku z otrzymaniem zgody na przetwarzanie danych należy podać osobie wszystkie informacje, których art. 13 RODO wymaga przy zbieraniu danych od osoby, której dane dotyczą. Proponowany wzór takich informacji podajemy osobno.

Załącznik nr 2a
do Polityka Ochrony Danych Osobowych w spółce Centro-chem sp. z o.o. sp.k.

Ogólna klauzula informacyjna

Zgodnie z art. 13 ust. 1−2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) – dalej RODO − informujemy, że:

Zgodnie z art. 13 ust. 1−2 oraz art. 26 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) – dalej RODO − informujemy, że:

I. Administratorzy danych osobowych

Spółkę Centro-chem sp. z o.o. sp.k., z siedzibą w Turce, Turka 141B, 20-258 Lublin, jest Administratorem Twoich danych osobowych.

II. Wspólne uzgodnienia między Administratorami

W ramach umowy o współadministrowanie, razem ze Współadministratorem uzgodniliśmy zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO, w szczególności uzgodniliśmy, że:

1. My, jako Administrator, jesteśmy odpowiedzialni za wykonanie wobec Ciebie obowiązku informacyjnego.
2. Spółka [.....], jako Współadministrator jest odpowiedzialna wobec Ciebie za umożliwienie Ci wykonywania Twoich praw. Niezależnie od tego ustalenia, możesz wykonywać swoje prawa również wobec nas. W takim przypadku przekażemy Twoje żądanie Współadministratorowi, który zrealizuje Twoje żądanie.
3. *(Należy uzupełnić jak najbardziej szczegółowo na podstawie umowy o współadministrowaniu).*

Treść uzgodnień pomiędzy nami a Współadministratorem znajduje się na stronie internetowej dostępnej pod adresem [.....].

III. Punkt kontaktowy

Razem ze Współadministratorem postanowiliśmy ustanowić wspólny punkt kontaktowy, z którym możesz się skontaktować w sprawach ochrony swoich danych osobowych pod emailem **…….** lub pisemnie na adres naszej siedziby wskazany w pkt I powyżej.

IV. Cele i podstawy przetwarzania

Wraz z Współadministratorem ustaliliśmy, cele przetwarzania Twoich danych. Będziemy przetwarzać Twoje dane:

(Poniżej znajdują się przykładowe cele oraz podstawy przetwarzania, które należy uzupełnić zgodnie z ustalonymi przez organizację czynnościami przetwarzania.)

1. w celu [.....] na podstawie Twojej zgody (podstawa z art. 6 ust. 1 lit. a RODO): W każdej chwili **przysługuje Ci prawo do wycofania zgody** na przetwarzanie Twoich danych osobowych, ale cofnięcie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie Twojej zgody przed jej wycofaniem.

   Czy wyrażasz zgodę na przetwarzanie Twoich danych osobowych zamieszczonych w niniejszym formularzu przez [.....] z siedzibą przy [.....] oraz przez [.....] z siedzibą przy [.....] w celu [.....]?

   □ TAK □ NIE

   (*Jeśli organizacje zbierają kilka zgód dot. różnych celów przetwarzania, zgody te muszą zostać wyrażone osobno. Niedozwolone jest zbiorcze zbieranie zgód.*)

2. w celu zawarcia umowy [.....] na podstawie Twojego zainteresowania naszą ofertą (podstawa z art. 6 ust. 1 lit. b RODO);
3. w celu wykonania i na podstawie umowy [X], gdy ją zawarliśmy (podstawa z art. 6 ust. 1 lit. b RODO);
4. w celu [.....], na podstawie obowiązku z art. [.....] ustawy o [.....] (*Sugerujemy jak najbardziej precyzyjne podanie podstawy prawnej, z której wynika obowiązek*) (podstawa z art. 6 ust. 1 lit. c RODO);
5. w celu [.....], ponieważ jest to niezbędne do ochrony Twoich żywotnych interesów lub żywotnych interesów innej osoby (*Sugerujemy wymienić, jakie to interesy, jeśli to możliwe.*) (podstawa z art. 6 ust. 1 lit. d RODO);
6. w celu [.....], ponieważ przetwarzanie jest niezbędne do wykonania zadania, które realizujemy w interesie publicznym (*Sugerujemy wymienić, jakie to zadanie)*/w ramach powierzonej nam władzy publicznej (podstawa z art. 6 ust. 1 lit. e RODO);
7. w celach analitycznych [lepszego doboru usług do potrzeb naszych klientów, ogólnej optymalizacji naszych produktów, optymalizacji procesów obsługi, budowania wiedzy o naszych klientach, analizy finansowej naszej spółki itp.] będącego realizacją naszego prawnie uzasadnionego w tym interesu (podstawa z art. 6 ust. 1 lit. f RODO);
8. w celach archiwalnych (dowodowych) będących realizacją naszego prawnie uzasadnionego interesu zabezpieczenia informacji na wypadek prawnej potrzeby wykazania faktów (art. 6 ust. 1 lit. f RODO);

9. w celu ewentualnego ustalenia, dochodzenia lub obrony przed roszczeniami będącego realizacją naszego prawnie uzasadnionego w tym interesu (podstawa z art. 6 ust. 1 lit. f RODO);
10. w celu badania satysfakcji klientów będącego realizacją naszego prawnie uzasadnionego interesu określania jakości naszej obsługi oraz poziomu zadowolenia naszych klientów z produktów i usług (podstawa z art. 6 ust. 1 lit. f RODO);
11. w celu oferowania Ci przez nas produktów i usług bezpośrednio (marketing bezpośredni), w tym dobierania ich pod kątem Twoich potrzeb, czyli profilowania, będącego realizacją naszego prawnie uzasadnionego w tym interesu (podstawa z art. 6 ust. 1 lit. f RODO);
12. w celu oferowania Ci bezpośrednio (marketing bezpośredni) produktów i usług firm z nami współpracujących (naszych partnerów), np. w formie kuponów rabatowych, w tym dobierania ich pod kątem Twoich potrzeb, czyli profilowania, będącego realizacją prawnie uzasadnionego w tym interesu naszego i naszych partnerów (podstawa z art. 6 ust. 1 lit. f RODO);

V. Prawo do sprzeciwu

1. W każdej chwili przysługuje Ci prawo do wniesienia sprzeciwu wobec przetwarzania Twoich danych na podstawie pkt IV.7−10 (*czyli tam, gdzie przywołujemy uzasadniony interes, ale z wyłączeniem marketingu bezpośredniego*) opisanych powyżej. Przestaniemy przetwarzać Twoje dane w tych celach, chyba że będziemy w stanie wykazać, że w stosunku do Twoich danych istnieją dla nas ważne prawnie uzasadnione podstawy, które są nadrzędne wobec Twoich interesów, praw i wolności lub Twoje dane będą nam niezbędne do ewentualnego ustalenia, dochodzenia lub obrony roszczeń.
2. W każdej chwili przysługuje Ci prawo do wniesienia sprzeciwu wobec przetwarzania Twoich danych w celu prowadzenia marketingu bezpośredniego. Jeżeli skorzystasz z tego prawa – zaprzestaniemy przetwarzania danych w tym celu.

VI. Okres przechowywania danych

1. Twoje dane osobowe wynikające z [zawarcia umowy X] będą przetwarzane przez okres, w którym mogą ujawnić się roszczenia związane z [tą umową], czyli przez [X]+1 lat od końca roku, w którym wygasła [umowa], w tym [X] lat to najdłuższy możliwy okres przedawnienia roszczeń, dodatkowy rok jest na wypadek roszczeń zgłoszonych w ostatniej chwili i problemów z doręczeniem, a liczenie od końca roku służy określeniu jednej daty usunięcia danych dla [umów] kończących się w danym roku.
2. Jeżeli nie dojdzie do [zawarcia umowy] w ciągu [X] od złożenia Ci przez nas oferty, Twoje dane osobowe związane z rozmowami o tej [umowie] zostaną niezwłocznie usunięte z wyjątkiem danych potrzebnych do marketingu bezpośredniego.

3. Dane przetwarzane dla potrzeb marketingu bezpośredniego naszych produktów i usług możemy przetwarzać do czasu, aż zgłosisz sprzeciw względem ich przetwarzania w tym celu lub ustalimy, że się zdezaktualizowały.

VII. Odbiorcy danych

Twoje dane osobowe mogą zostać ujawnione: [podmiotom z naszej grupy kapitałowej; naszym partnerom, czyli firmom, z którymi współpracujemy łącząc produkty lub usługi itp.] (*Proszę jak najdokładniej opisać wymienionych odbiorców*).

Do Twoich danych mogą też mieć dostęp nasi podwykonawcy (podmioty przetwarzające), np. firmy księgowe, prawnicze, informatyczne, likwidatorzy szkód, wykonawcy usług w ramach likwidacji szkód, agencje marketingowe (*Proszę jak najdokładniej opisać wymienione podmioty przetwarzające*).

VIII. Prawa osób, których dane dotyczą:

Zgodnie z RODO, przysługuje Ci:

a) prawo dostępu do swoich danych oraz otrzymania ich kopii;
b) prawo do sprostowania (poprawiania) swoich danych;
c) prawo do usunięcia danych, ograniczenia przetwarzania danych;
d) prawo do wniesienia sprzeciwu wobec przetwarzania danych;
e) prawo do przenoszenia danych;
f) prawo do wniesienia skargi do organu nadzorczego.

IX. Informacja o wymogu/dobrowolności podania danych

Podanie danych jest obowiązkiem wynikającym z art. [.....] ustawy o [.....] i stanowi warunek [zawarcia umowy].

(*lub*)

Podanie danych ma charakter dobrowolny, [ale jest konieczne do zawarcia umowy itp.].

X. Zautomatyzowane podejmowanie decyzji

W procesie [analizy ryzyka/wykonywania umowy] podejmujemy decyzje w sposób zautomatyzowany, z uwzględnieniem profilowania, w oparciu o dane [podane w niniejszym formularzu]. Decyzje te są podejmowane całkowicie automatycznie w oparciu o [modele scoringowe/analizy statystyczne/metody oceny ryzyka itp.]. Decyzje podejmowane w ten zautomatyzowany sposób mają wpływ na [wysokość opłaty/składki, dostępność produktów itp.].

Profilowanie oznacza przetwarzanie danych osobowych polegające na wykorzystaniu Twoich danych osobowych do oceny niektórych Twoich cech, w szczególności do analizy lub prognozy aspektów dotyczących Twoich efektów pracy, sytuacji ekonomicznej,

zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Podejmowanie decyzji w sposób zautomatyzowany do celów [.....] jest niezbędne do celu zawarcia lub wykonania łączącej nas umowy.

(*lub*)

Podejmowanie decyzji w sposób zautomatyzowany do celów [.....] odbywa się zgodnie z art. [.....] ustawy o [.....].

(*lub*)

Podejmowanie decyzji w sposób zautomatyzowany do celów [.....] odbywa się na podstawie udzielonej przez Ciebie zgody.

Załącznik nr 3
do Polityka Ochrony Danych Osobowych w spółce Centro-Chem Sp. z o.o. Sp.k.

Ewidencja osób upoważnionych do przetwarzania danych osobowych

L.p.	Imię i Nazwisko	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia	Login/ Identyfikator w systemie informatycznym	Uwagi
1.						
2.						
3.						
…						

Załącznik nr 4
do Polityka Ochrony Danych Osobowych w spółce Centro-Chem Sp. z o.o. Sp.k.

Rejestr Czynności Przetwarzania Danych Osobowych

Rejestr czynności przetwarzania – przykład		
Administrator i jego dane kontaktowe:	**Spółka Centro-Chem Sp. z o.o. Sp.k., Turka 141B, 20-258 Lublin, adres e-mail: info@centro-chem.pl.**	
Dane inspektora ochrony danych lub osoby odpowiedzialnej za ochronę danych osobowych u administratora, jeżeli została wyznaczona:	**……**	
Osoba odpowiedzialna za aktualizację rejestru:	**…….**	
Nazwa procesu (Nazwa czynności przetwarzania):	**Rekrutacja pracowników** **Numer wpisu:** *(poszczególne procesy wymagają osobnego ujęcia w analogicznej formie)*	
Cel przetwarzania danych:	*Opisać cel przetwarzania w procesie np. wyłonienie spośród kandydatów na określone stanowisko, osoby, która możliwie najdokładniej spełni oczekiwania administratora wobec przyszłego pracownika - pod kątem zarówno umiejętności, kompetencji miękkich, nastawienia do firmy, jak i oczekiwań finansowych.*	
Charakter przetwarzania danych:	*Opisać planowane lub realizowane operacje przetwarzania, rodzaje danych osobowych, które mają być przetwarzane, w tym to czy będą przetwarzane dane wrażliwe.*	
Podstawa przetwarzania	*opisać podstawę przetwarzania, na której oparto proces, np. zgoda kandydata.*	
Kategorie osób, których dane dotyczą	*opisać zaangażowane w proces podmioty* np. ✓ pracownicy obsługujący proces, ✓ kontrahenci obsługujący proces oraz ich pracownicy, ✓ kandydaci do pracy,	
Zakres przetwarzanych danych według kategorii danych: (*wskazano przykładowy zakres*)	Dane identyfikacyjne	• imię (imiona) i nazwisko; • imiona rodziców kandydata do pracy; • data urodzenia kandydata do pracy ; • PESEL

	Dane kontaktowe	• telefon kontaktowy; • adres zameldowania; • adres do korespondencji;
	Dane dotyczące przebiegu kariery i wykształcenia, oczekiwań wobec pracodawcy	• wykształcenie (nazwa szkoły, rok ukończenia szkoły, zawód, specjalność, stopień naukowy, tytuł zawodowy, tytuł naukowy); • wykształcenie uzupełniające (kursy, studia podyplomowe, data ukończenia nauki); • przebieg dotychczasowego zatrudnienia (nazwa pracodawcy, stanowisko pracy, okres zatrudnienia od – do); • oczekiwania finansowe; • wyniki przeprowadzonych testów kompetencji;
	Dane dotyczące dodatkowych uprawnień	• dodatkowe uprawnienia, umiejętności, zainteresowania (np. stopień znajomości języków obcych, prawo jazdy, uprawnienia zawodowe);
Kontekst przetwarzanych danych:	*Opisać wszelkie okoliczności prawne i faktyczne przetwarzania. Przede wszystkim należy oceniać intensywność ingerencji w prywatność danego procesu przetwarzania danych, używanych narzędzi i dostępnej technologii, okoliczności i sposób wykorzystywania założonego rozwiązania i relacji do pozostałych elementów ocennych, w tym celu przetwarzania, a także przesłanek legalizacyjnych. Relewantne mogą również być czas i długość przetwarzania.*	
Kategorie odbiorców / Odbiorcy danych	*Wskazać kategorie odbiorców ewentualnie konkretne podmioty, którym ujawniono lub zostaną ujawnione dane, w tym z państw trzecich, z podziałem na podmioty przetwarzające (np. agencje rekrutacyjne) i innych odbiorców jeśli występują w danym procesie.*	
Współadministrowanie	*Opis współadministrowania, podziału obowiązków oraz dane współadministratora, w tym dane kontaktowe.*	
Transfery danych	*Przekazania danych do państw trzecich lub organizacji międzynarodowych, ze wskazaniem podstawy, na której oparto transfer oraz jeśli jest to przypadek, o którym mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń.*	
Retencja	*Wskazać okresy przechowywania i planowane terminy usunięcia.* *Opisać proces usuwania danych po osiągnięciu celu oraz procedurę ewentualnej zmiany celu.*	

Opis środków technicznych i organizacyjnych	*Opisać zabezpieczenia procesu, fizyczne, organizacyjne, osobowe, techniczne przez pryzmat poufności, integralności i dostępności:* *Np.* *1. Zabezpieczenia organizacyjne:* *a) Upoważnienia do przetwarzania danych* *b) Oświadczenie o zachowaniu poufności* *c) Szkolenie z zakresu ochrony danych* *d) Podpisanie umowy powierzenia* *e) Dokonywanie przeglądów stosowanych procedur* *f) Wdrożenie odpowiednich polityk retencyjnych* *g) Wdrożenie odpowiednich polityk informacyjnych* *2. Zabezpieczenia informatyczne i fizyczne:* *a) anonimizacja, usuwanie danych* *b) backupy danych* *c) blokada USB, napędów optycznych* *d) indywidualne konta w systemie operacyjnym / indywidualne konta w programach przetwarzających dane* *e) legalność oprogramowania* *f) logowanie operacji na danych osobowych* *g) niszczenie nośników / niszczenie wydruków* *h) ochrona przed zanikiem zasilania* *i) lokalizacja stanowisk komputerowych* *j) polityka kluczy - dostęp do pomieszczeń* *k) postępowanie z komputerami przenośnymi* *l) poziomy uprawnień w programach (użytkowników)* *m) poziomy uprawnień administratorów (serwery)* *n) procedura korzystania z poczty elektronicznej / procedura korzystania z Internetu / procedury pracy przy stanowisku komputerowym* *o) programy antywirusowe, firewalle*

<table>
<tr><td></td><td colspan="2">p) szyfrowanie transmisji / szyfrowanie dysków / szyfrowanie plików zapisywanych na nośnikach

q) wydzielone miejsca przechowywania dokumentów i nośników danych</td></tr>
<tr><td>Prawdopodobieństwo naruszenia praw podmiotów danych skumulowana analiza PID (poufność, integralność, dostępność):

Skala:

1 pkt = niska możliwość wystąpienia nie zachodzi (3-4 punktów PID)

2 pkt = średna możliwość wystąpienia wynika za splotu niezależnych od siebie i administratora czynników (5-6 punktów PID)

3 pkt = wysoka możliwość wystąpienia co do zasady zachodzi (7-9 punktów PID)

4 pkt = bardzo wysoka możliwość wystąpienia jest przewidywalna i możliwa do opisania co do przyczyn (10-12 punktów PID)</td><td colspan="2">Opisać i dokonać oceny prawdopodobieństwa naruszenia praw podmiotów danych, według przyjętej metodologii.

Ocena uwzględnia według przyjętej metodologii:

Brak zapewnienia poufności (możliwość ujawienia lub nieuprawnionego dostępu), integralności (możliwość dekompilacji, modyfikacji) i dostępności (możliwości zarówno przypadkowego, jak i umyślnego zniszczenie lub usunięcie) powodujący duże prawdopodobieństwo utraty kontroli nad własnymi danymi skutkujące dla podmiotu danych możliwością powstania szkód majątkowych i niemajątkowych, w tym kradzieży tożsamości, dyskryminacji ze względu na dane szczególnych kategorii dotyczące stanu zdrowia.

<u>Poufność (1-4)</u>

Np. Bardzo wysokie –

Polegające na ….

<u>Integralność (1-4)</u>

Bardzo wysokie –

Polegające na ….

<u>Dostępność (1-4)</u>

Bardzo wysokie –

Polegające na …

SUMARYCZNIE …..pkt</td></tr>
<tr><td rowspan="4">Waga Naruszenia (Istotność naruszenia z perspektywy prywatności wg kategorii danych)

Skala 2-16 (wykładniczo)</td><td>Dane identyfikacyjne</td><td>Określić wagi poszczególnych danych, np. 2,4,8,16 itd. – zależnie od oceny intensywności wpływu na prywatność poszczególnych kategorii danych osobowych</td></tr>
<tr><td>Dane kontaktowe</td><td></td></tr>
<tr><td>Dane dotyczące przebiegu kariery i wykształcenia, oczekiwań wobec pracodawcy</td><td></td></tr>
<tr><td>Dane dotyczące dodatkowych uprawnień</td><td></td></tr>
</table>

<table>
<tr><td></td><td>Dane dotyczące stanu zdrowia</td><td></td></tr>
<tr><td rowspan="4">Poziom prawdopodobieństwa wystąpienia ryzyka naruszenia praw podmiotów danych z uwzględnieniem Wag Naruszenia poszczególnych kategorii danych

Iloczyn Prawdopodobieństwa oraz Wagi Naruszenia</td><td>Dane identyfikacyjne</td><td>Dokonać obliczeń (Iloczyn Prawdopodobieństwa oraz Wagi Naruszenia)</td></tr>
<tr><td>Dane kontaktowe</td><td></td></tr>
<tr><td>Dane dotyczące przebiegu kariery i wykształcenia, oczekiwań wobec pracodawcy</td><td></td></tr>
<tr><td>Dane dotyczące dodatkowych uprawnień</td><td></td></tr>
<tr><td>Ocena zasadności dokonania w procesie oceny skutków dla ochrony danych</td><td colspan="2">Dokonać oceny zaistnienia poniższych wymogów:

Ocenę skutków dla ochrony danych przeprowadza się:

a) jeżeli dany rodzaj przetwarzania - w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych,
b) w przypadku dokonywania przez administratora systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
c) w przypadku dokonywania przez administratora przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10; lub
d) w przypadku dokonywania przez administratora systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.
Zgodnie z Wytycznymi Grupy Roboczej art. 29 dotyczącymi oceny skutków dla ochrony danych oraz pomagającymi ustalić, czy przetwarzanie „może powodować wysokie ryzyko” do celów rozporządzenia 2016/679 (WP 248 rev.01) administrator może uznać konieczność przeprowadzenia oceny skutków jeśli występują dwa z poniższych czynników:

• Ocena lub punktacja, w tym profilowanie i prognozowanie w szczególności na podstawie „aspektów dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą” (motywy 71 i 91).
• Automatyczne podejmowanie decyzji o skutku prawnym lub podobnie znaczącym skutku: przetwarzanie mające na celu podjęcie decyzji w sprawie osób, których dane dotyczą, wywołujących „skutki prawne wobec osoby fizycznej” lub decyzji, które „w podobny sposób istotnie na nią wpływają” (art. 35 ust. 3 lit. a).
• Systematyczne monitorowanie: przetwarzanie wykorzystywane do obserwacji, monitorowania lub kontrolowania osób, których dane dotyczą, w tym danych gromadzonych za pośrednictwem sieci lub ramach „systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie” (art. 35 ust. 3 lit. c).</td></tr>
</table>

	• *Dane wrażliwe lub dane o charakterze wysoce osobistym: obejmują szczególne kategorie danych osobowych określone w art. 9 (np. informacje o poglądach politycznych obywateli) oraz dane osobowe dotyczące wyroków skazujących za przestępstwo lub naruszeń prawa, zdefiniowane w art. 10.* • *Dane przetwarzane na dużą skalę: w RODO nie zawarto definicji pojęcia „przetwarzanie na dużą skalę", choć w motywie 91 przedstawiono pewne wskazówki w tym zakresie. W każdym razie Grupa Robocza Art. 29 zaleca, aby przy ustalaniu, czy przetwarzanie danych odbywa się na dużą skalę, wziąć pod uwagę w szczególności następujące czynniki:* *a) liczbę osób, których dane dotyczą – wyrażoną jako konkretna wartość albo jako odsetek populacji odniesienia;* *b) ilość danych lub zakres poszczególnych przetwarzanych pozycji danych;* *c) czas trwania lub trwałość czynności przetwarzania danych;* *d) zakres geograficzny czynności przetwarzania.* • *Dopasowywanie lub łączenie zbiorów danych np. pochodzących z co najmniej dwóch operacji przetwarzania danych przeprowadzonych w różnych celach lub przez różnych administratorów danych w sposób wykraczający poza uzasadnione oczekiwania osób, których dane dotyczą.* • *Dane dotyczące osób wymagających szczególnej opieki, których dane dotyczą (zob. motyw 75): przetwarzanie tego rodzaju danych stanowi jedno z kryteriów ze względu na zwiększoną nierównowagę sił miedzy osobami, których dane dotyczą, a administratorem danych, co oznacza, że osoby fizyczne mogą mieć trudności z wyrażeniem zgody na przetwarzanie swoich danych lub z wyrażeniem sprzeciwu wobec ich przetwarzania, lub mogą mieć trudności z korzystaniem z przysługujących im praw. Do osób wymagających szczególnej opieki, których dane dotyczą, można zaliczyć dzieci (można je uznać za niezdolne do świadomego i przemyślanego sprzeciwienia się przetwarzaniu danych lub do wydrążenia zgody na przetwarzanie danych), pracowników, bardziej wrażliwe grupy społeczne wymagające szczególnej ochrony (osoby chore psychicznie, osoby ubiegające się o azyl lub osoby starsze, pacjenci itp.) oraz każdą sytuację, gdy można stwierdzić brak równowagi miedzy stanowiskiem osoby, której dane dotyczą, a stanowiskiem administratora.* • *Innowacyjne wykorzystanie lub stosowanie nowych rozwiązań technologicznych lub organizacyjnych, takich jak połączenie technologii rozpoznającej odcisk palca i twarz w celu poprawy fizycznej kontroli dostępu itd. W RODO (art. 35 ust. 1 i motywy 89 i 91) wyjaśniono, że wykorzystanie nowej technologii zdefiniowanej „zgodnie ze stanem wiedzy technicznej" (motyw 91) może sprawić, iż konieczne będzie przeprowadzenie oceny skutków dla ochrony danych. Wynika to z tego, że zastosowanie takiej technologii może wiązać się z nowymi formami gromadzenia i wykorzystania danych, co może stwarzać ryzyko naruszenia praw i wolności osób fizycznych. W istocie osobiste i społeczne skutki wprowadzenia nowej technologii*

	mogą nie być znane. Ocena skutków dla ochrony danych pomoże administratorowi danych zrozumieć takie ryzyko i je wyeliminować. • *Gdy samo przetwarzanie „uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy" (art. 22 i motyw 91). Obejmuje to operacje przetwarzania, których celem jest umożliwienie osobom, których dane dotyczą, uzyskania dostępu do usługi lub zawarcia umowy, zmiana tego dostępu lub odmówienie dostępu.*
Uprzednie konsultacje	*Wskazać na przeprowadzenie i wynik uprzednich konsultacji z organem nadzorczym*
Zastosowanie kodeksu dobrych postępowania	*Wskazać stosowany kodeks postępowania zatwierdzony przez organ nadzorczy, z odniesieniem do jego zastosowania w procesie*
Informacje dodatkowe np. podleganiu certyfikacji w procesie lub jego części	*Wskazać podleganie certyfikacji i opisać zakres uzyskanego certyfikatu*

Załącznik nr 5
do Polityka Ochrony Danych Osobowych w spółce Centro-Chem Sp. z o.o. Sp.k.

REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA

Lp.	Kategorie przetwarzań	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (*jeżeli to możliwe*)	Administrator				Czas trwania przetwarzania	Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane	Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi	Podprzetwarzający (podwykonawca) (*jeśli dotyczy*)	
			Nazwa i dane Administratora	Nazwa i dane kontaktowe współadministratora (*jeśli dotyczy*)	Nazwa i dane kontaktowe przedstawiciela administratora (*jeśli wyznaczono*)	Inspektor Ochrony Danych Administratora (*jeśli powołano*)				Nazwa i dane kontaktowe podprzetwarzającego (podwykonawcy)	Kategorie podpowierzonych przetwarzań
	Art. 30 ust. 2b	Art. 30 ust. 2d, art. 32 ust. 1	Art. 30 ust. 2a					Art. 30 ust. 2c	Art. 30 ust. 2c		
	1	2	3	4	5	6	7	8	9	10	11

Załącznik nr 6
do Polityka Ochrony Danych Osobowych w spółce Centro-Chem Sp. z o.o. Sp.k.

Zgłoszenie naruszenia ochrony danych osobowych

1. Typ zgłoszenia

Wskaż czy zgłaszasz naruszenie ochrony danych osobowych mające charakter jednorazowego zdarzenia (np. zgubienie, kradzież nośnika danych, przypadkowe wysłanie danych osobie nieuprawnionej), czy przygotowujesz wstępne zgłoszenie, które uzupełnisz później, lub czy uzupełniasz lub zmieniasz wcześniejsze zgłoszenie.

Podaj swoją sygnaturę sprawy (opcjonalnie)
(np. sygnatura w Twoim wewnętrznym rejestrze naruszeń) Kliknij tutaj, aby wprowadzić tekst.

◉ Zgłoszenie kompletne/jednorazowe	○ Zgłoszenie wstępne	○ Zgłoszenie uzupełniające/zmieniające
	Podaj przybliżoną datę uzupełnienia zgłoszenia (opcjonalnie) Kliknij tutaj, aby wprowadzić datę.	Podaj datę poprzedniego zgłoszenia (opcjonalnie) Kliknij tutaj, aby wprowadzić datę. Podaj sygnaturę sprawy UODO Kliknij tutaj, aby wprowadzić tekst.

☐ Naruszenie zostało lub zostanie zgłoszone organowi ochrony danych osobowych w innym państwie Jeśli tak, podaj w jakim.

☐ Naruszenie zostało lub zostanie zgłoszone innym organom np. Policja, CSIRT NASK, CSIRT GOV, CSIRT MON (najedź myszką na nazwę organu by dowiedzieć się więcej)

Podaj nazwy tych organów Kliknij tutaj, aby wprowadzić tekst.

Podaj numer/sygnaturę zgłoszenia do innego organu Kliknij tutaj, aby wprowadzić tekst.

2. Podmiot zgłaszający

2A. Dane administratora danych

Pełna nazwa administratora Kliknij tutaj, aby wprowadzić tekst.

REGON (opcjonalnie) Podaj numer. NIP (opcjonalnie) Podaj numer. KRS (opcjonalnie) Podaj numer.

Sektor (opcjonalnie)	*Dla sektora publicznego:* Wybierz element.		*Dla sektora prywatnego:* Wybierz element.		
2B. Adres siedziby administratora danych					
Ulica	Kliknij tutaj, aby wprowadzić tekst.	Numer domu	Podaj numer	Numer lokalu	Podaj numer
Miejscowość	Kliknij tutaj, aby wprowadzić tekst.	Kod pocztowy	Kliknij tutaj, aby wprowadzić tekst.		
Gmina	Kliknij tutaj, aby wprowadzić tekst.	Powiat	Kliknij tutaj, aby wprowadzić tekst.		
Województwo	Kliknij tutaj, aby wprowadzić tekst.	Państwo	Kliknij tutaj, aby wprowadzić tekst.		
2C. Osoby uprawnione do reprezentowania administratora					
	Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.	
(Aby dopisać kolejne osoby, należy po kliknięciu na powyższe pole kliknąć przycisk , który pojawi się po prawej stronie)					
2D. Pełnomocnik					
☐ Wniosek wypełniany przez pełnomocnika (opcjonalnie)					
Jeśli zgłoszenie przesyłane jest w formie elektronicznej, należy załączyć pełnomocnictwo **udzielone w formie elektronicznej** oraz dowód uiszczenia opłaty skarbowej					
2E. Inspektor ochrony danych					
Imię i nazwisko	imię i nazwisko.	Numer telefonu	Numer telefonu.	Adres e-mail	E-mail.
☐ Inspektor nie został wyznaczony					
Jeśli inspektor nie został wyznaczony podaj dane innego punktu kontaktowego, od którego można uzyskać więcej informacji o naruszeniu. Kliknij tutaj, aby wprowadzić tekst.					
2F. Inne podmioty uczestniczące w przetwarzaniu danych, których dotyczy naruszenie (opcjonalnie)					
Podaj nazwy podmiotów, dane kontaktowe i wyjaśnij ich rolę w procesie przetwarzania, którego dotyczy naruszenie (np. podmiot przetwarzający, współadministratora, operator pocztowy itp.)					

1.	Nazwa i dane kontaktowe	Kliknij tutaj, aby wprowadzić tekst.	Rola	Kliknij tutaj, aby wprowadzić tekst.

(Aby dopisać kolejne podmioty, należy po kliknięciu na powyższe pole kliknąć przycisk , który pojawi się po prawej stronie)

2. Czas naruszenia

3A. Wykrycie naruszenia i powiadomienie organu nadzorczego

Data stwierdzenia naruszenia
Wskaż kiedy dowiedziałeś/aś się o naruszeniu.
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.
Kliknij tutaj, aby wprowadzić datę.

Sposób stwierdzenia naruszenia
Np. zgłoszenie osoby której dane dotyczą czy cykliczny przegląd logów systemowych zgodnie z wdrożoną polityką bezpieczeństwa

Kliknij tutaj, aby wprowadzić tekst.

Data powiadomienia przez podmiot przetwarzający
(opcjonalnie)
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.
Kliknij tutaj, aby wprowadzić tekst.

Powody opóźnienia powiadomienia organu nadzorczego o naruszeniu
Pole obowiązkowe jeśli czas od momentu stwierdzenia naruszenia do czasu wypełniania formularza jest dłuższy niż 72h

Kliknij tutaj, aby wprowadzić tekst.

3B. Czas naruszenia

Data i czas zaistnienia/rozpoczęcia naruszenia
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.
Kliknij tutaj, aby wprowadzić tekst.

Data i czas zakończenia naruszenia
(opcjonalnie)
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.
Kliknij tutaj, aby wprowadzić tekst.

3. Charakter naruszenia

4A. Opisz szczegółowo na czym polegało naruszenie

Kliknij tutaj, aby wprowadzić tekst.

4B. Na czym polegało naruszenie?

☐ a) Zgubienie lub kradzież nośnika/urządzenia

☐ b) Dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji

☐ c) Korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem jej do nadawcy

☐ d) Nieuprawnione uzyskanie dostępu do informacji

☐ e) Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń

☐ f) Złośliwe oprogramowanie ingerujące w poufność, integralność lub dostępność danych

☐ g) Uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (phishing)

☐ h) Nieprawidłowa anonimizacja danych osobowych w dokumencie

☐ i) Nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora

☐ j) Niezamierzona publikacja

☐ k) Dane osobowe wysłane do niewłaściwego odbiorcy

☐ l) Ujawnienie danych niewłaściwej osoby

☐ m) Ustne ujawnienie danych osobowych

4C. Działanie złośliwego oprogramowania (odpowiedz na poniższe pytania, jeśli w sekcji 4B zaznaczono pole f)

1. Jeśli w ocenie administratora doszło wyłącznie do naruszenia dostępności danych, w jaki sposób stwierdzono, że nie doszło do naruszenia ich poufności? (w sytuacji gdy np. dane nie zostały pobrane przez osobę nieupoważnioną, a jedynie zaszyfrowane w sposób uniemożliwiający uzyskanie do nich dostępu)

Kliknij tutaj, aby wprowadzić tekst.

2. Czy, a jeżeli tak, to w jakiej formie, złośliwe oprogramowanie poinformowało o konieczności uiszczenia opłaty w celu odzyskania dostępu do danych (podaj nazwę złośliwego oprogramowania, sposób poinformowania, żądaną kwotę, kanał komunikacji, sposób zapłaty oraz termin)

Kliknij tutaj, aby wprowadzić tekst.

3. Jeżeli doszło do utraty dostępności danych, to czy administrator był w posiadaniu kopii zapasowej, jeśli tak to w jakim czasie ją przywrócił?

Kliknij tutaj, aby wprowadzić tekst.

UWAGA: *Jeżeli zgłoszenie naruszenia dotyczy podejrzanych załączników, phishingu, szantażu czy działania złośliwego oprogramowania, rozważ zgłoszenie zdarzenia do CERT Polska pod adresem https://incydent.cert.pl/. Dokonanie takiego zgłoszenia jest szczególnie zalecane w przypadku, kiedy odpowiedzi na powyższe pytania są utrudnione bądź niemożliwe.*
O fakcie zgłoszenia incydentu do CERT Polska poinformuj w zgłoszeniu uzupełniającym Prezesa UODO (pkt 1 formularza) podając datę zgłoszenia, jego numer oraz ewentualnie informacje na temat incydentu otrzymane od CERT Polska).

4D. Przyczyna naruszenia

☐ Wewnętrzne działanie niezamierzone ☐ Wewnętrzne działanie zamierzone

☐ Zewnętrzne działanie niezamierzone ☐ Zewnętrzne działanie zamierzone

4E. Charakter

☐ Naruszenie poufności danych
Nieuprawnione lub przypadkowe ujawnienie bądź udostępnienie danych

☐ Naruszenie integralności danych
Wprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub przechowywania

☐ Naruszenie dostępności danych
Brak możliwości wykorzystania danych na żądanie, w założonym czasie, przez osobę do tego uprawnioną

4F. Dzieci

☐ Naruszenie dotyczy przetwarzania danych w związku ze świadczeniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.
(opcjonalnie)

4. Liczba osób i wpisów

Przybliżona liczba osób, których dotyczy naruszenie

Kliknij tutaj, aby wprowadzić tekst.

Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie
Nie dotyczy to liczby osób. Jednej osobie można przypisać kilka wpisów (np. jednej osobie można przypisać kilka wykonanych transakcji)

Kliknij tutaj, aby wprowadzić tekst.

5. Kategorie danych osobowych

UWAGA: W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.

6A. Dane podstawowe

☐ Nazwiska i imiona
☐ Imiona rodziców
☐ Data urodzenia
☐ Numer rachunku bankowego
☐ Adres zamieszkania lub pobytu
☐ Numer ewidencyjny PESEL
☐ Adres e-mail
☐ Nazwa użytkownika i/lub hasło
☐ Dane dotyczące zarobków i/lub posiadanego majątku
☐ Nazwisko rodowe matki
☐ Seria i numer dowodu osobistego
☐ Numer telefonu
☐ Wizerunek
☐ Inne, wskaż jakie:

Kliknij tutaj, aby wprowadzić tekst.

6B. Dane szczególnej kategorii

☐ Dane o pochodzeniu rasowym lub etnicznym
☐ Dane o poglądach politycznych
☐ Dane o przekonaniach religijnych lub światopoglądowych
☐ Dane o przynależności do związków zawodowych
☐ Dane dotyczące seksualności lub orientacji seksualnej
☐ Dane dotyczące zdrowia
☐ Dane genetyczne
☐ Dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej

6C. Dane, o których mowa w art. 10 RODO

☐ Dane dotyczące wyroków skazujących
☐ Dane dotyczące czynów zabronionych
☐ Inne
Kliknij tutaj, aby wprowadzić tekst.

6. Kategorie osób

☐ Pracownicy
☐ Użytkownicy
☐ Subskrybenci
☐ Studenci
☐ Uczniowie
☐ Służby mundurowe (np. wojsko, policja)
☐ Klienci (obecni i potencjalni)
☐ Klienci podmiotów publicznych
☐ Pacjenci
☐ Dzieci
☐ Osoby o szczególnych potrzebach (np. osoby starsze, niepełnosprawne itp.)

Szczegółowy opis kategorii osób, których dotyczy naruszenie:
Opisz np. kogo i w jakim przedziale czasowym dotyczy naruszenie
W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.
Kliknij tutaj, aby wprowadzić tekst.

7. Możliwe konsekwencje

8A. Uszczerbek fizyczny, majątkowy, niemajątkowy lub inne znaczące konsekwencje dla osoby, której dane dotyczą

☐ Utrata kontroli nad własnymi danymi osobowymi
☐ Ograniczenie możliwości realizowania praw z art. 15-22 RODO
☐ Ograniczenie możliwości realizowania praw
☐ Dyskryminacja
☐ Kradzież lub sfałszowanie tożsamości
☐ Strata finansowa
☐ Naruszenie dobrego imienia
☐ Utrata poufności danych osobowych chronionych tajemnicą zawodową
☐ Nieuprawnione odwrócenie pseudonimizacji
☐ Inne

Opisz poniżej inne skutki naruszenia prawa do ochrony danych osoby, której dane dotyczą:

Kliknij tutaj, aby wprowadzić tekst.

8B. Czy wystąpiło wysokie ryzyko naruszenia praw lub wolności osób fizycznych?

◉ Tak ○ Nie

Uzasadnienie

Kliknij tutaj, aby wprowadzić tekst.

8. Środki bezpieczeństwa i środki zaradcze

9A. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa dotychczas stosowanych

Kliknij tutaj, aby wprowadzić tekst.

9B. Środki bezpieczeństwa zastosowane lub proponowane w celu zminimalizowana ryzyka ponownego wystąpienia naruszenia

Kliknij tutaj, aby wprowadzić tekst.

9C. Środki zastosowane lub proponowane w celu zaradzenia naruszeniu i zminimalizowania negatywnych skutków dla osób, których dane dotyczą

Kliknij tutaj, aby wprowadzić tekst.

Czy osoby, których dane dotyczą, zostały zawiadomione o naruszeniu?

◉ Tak	○ Nie, ale zostaną zawiadomione Pamiętaj, że po powiadomieniu osób, należy przesłać treść zawiadomienia do UODO.	○ Nie, nie zostaną zawiadomione, ponieważ:	○ Nie oceniłem jeszcze

Czy indywidualnie?

◉ Tak

○ Nie, gdyż indywidualne zawiadomienie każdej osoby, której dane dotyczą wymagałoby niewspółmiernie dużego wysiłku. W związku z tym został bądź zostanie wydany publiczny komunikat lub zastosowany podobny środek, za pomocą którego osoby, których dane dotyczą, zostały bądź zostaną poinformowane w równie skuteczny sposób.

Wskaż datę zawiadomienia

Kliknij tutaj, aby wprowadzić datę.

Wskaż datę planowanego zawiadomienia

Kliknij tutaj, aby wprowadzić datę.

Liczba zawiadomionych osób

Kliknij tutaj, aby wprowadzić tekst.

☐ Nie znam jeszcze daty kiedy zamierzam zawiadomić osoby, których dane dotyczą

Środki komunikacji wykorzystane do zawiadomienia osoby, której dane dotyczą

Kliknij tutaj, aby wprowadzić tekst.

Umieść zanonimizowaną treść zawiadomienia, którą przesłałeś bądź zamierzasz przesłać do osób, których dane dotyczą.

Pamiętaj, że zawiadomienie powinno:

1. opisywać jasnym i prostym językiem charakter naruszenia ochrony danych osobowych,
2. zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
3. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
4. opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Kliknij tutaj, aby wprowadzić tekst.

○ przed naruszeniem wdrożono odpowiednie techniczne i organizacyjne środki ochrony (wskazane w pkt. 9A formularza) i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, anonimizacja czy pseudonimizacja uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych.

○ po naruszeniu zastosowano środki (wskazane w pkt. 9C formularza) eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą.

○ stwierdzono brak wysokiego ryzyka naruszenia praw lub wolności osób fizycznych (uzasadnienie w pkt. 8B formularza).

Jeśli jeszcze nie oceniłeś, czy zamierzasz zawiadomić osoby, których dane dotyczą, pamiętaj, że po podjęciu takiej decyzji będziesz musiał złożyć zgłoszenie uzupełniające.

5. Przetwarzanie transgraniczne

☐ Naruszenie ma charakter transgraniczny

Zaznacz kraje Europejskiego Obszaru Gospodarczego, których dotyczy naruszenie:

☐ Austria	☐ Belgia	☐ Bułgaria	☐ Chorwacja
☐ Cypr	☐ Czechy	☐ Dania	☐ Estonia
☐ Finlandia	☐ Francja	☐ Grecja	☐ Hiszpania
☐ Holandia	☐ Irlandia	☐ Islandia	☐ Liechtenstein
☐ Litwa	☐ Luksemburg	☐ Łotwa	☐ Malta
☐ Niemcy	☐ Norwegia	☐ Portugalia	☐ Rumunia
☐ Słowacja	☐ Słowenia	☐ Szwecja	☐ Węgry
☐ Wielka Brytania	☐ Włochy		

_____

Data, miejscowość
(dla zgłoszenia w formie papierowej)

_____

Podpis osoby lub osób upoważnionych
do reprezentowania administratora[5]
(dla zgłoszenia w formie papierowej)

[5] Jeżeli zgłoszenie podpisuje pełnomocnik, należy pamiętać o załączeniu pełnomocnictwa

Informacja:

Administrator danych osobowych.
Administratorem Państwa danych osobowych będzie Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO) z siedzibą w Warszawie, przy ul. Stawki 2.

Można się z nami kontaktować w następujący sposób:
a) listownie: ul. Stawki 2, 00-193 Warszawa
b) przez elektroniczną skrzynkę podawczą dostępną na stronie https://www.uodo.gov.pl/pl/p/kontakt
c) telefonicznie: (22) 531 03 00

Inspektor ochrony danych.
Możecie się Państwo kontaktować również z wyznaczonym przez Prezesa UODO inspektorem ochrony danych pod adresem email IOD@uodo.gov.pl

Cele i podstawy przetwarzania.
Będziemy przetwarzać Państwa dane osobowe zawarte w formularzu w celu przyjmowania zgłoszeń o naruszeniu ochrony danych osobowych zgodnie z art. 33 ust 1 , 3 i 4 RODO[1] bądź art. 44 ust. 1 – 5 DODO[2], podejmowania działań określonych w art. 34 ust. 4 oraz art. 58 ust. 2 RODO bądź art. 45 ust. 5 DODO, a także prowadzenia przez organ wewnętrznego rejestru naruszeń na podstawie art. 57 ust. 1 lit. u RODO. Następnie Państwa dane będziemy przetwarzać w celu wypełnienia obowiązku archiwizacji dokumentów wynikającego z ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.

Odbiorcy danych osobowych.
Odbiorcami Państwa danych osobowych będą Minister Cyfryzacji w związku z zamieszczeniem formularza na platformie E-PUAP bądź Minister Przedsiębiorczości i Technologii w związku z zamieszczeniem formularza na platformie biznes.gov.pl

Okres przechowywania danych.
Będziemy przechowywać Państwa dane przez czas realizacji uprawnień Prezesa UODO wskazanych w art. 34 ust. 4 RODO i art. 58 ust. 2 RODO bądź art. 45 ust. 5 DODO, a następnie - zgodnie z obowiązującą w Urzędzie Prezesa UODO Instrukcją kancelaryjną oraz przepisami o archiwizacji dokumentów - przez okres 10 lat od końca roku, w którym zgłoszono naruszenie ochrony danych, lub - w przypadku skierowania wystąpienia lub wydania decyzji administracyjnej – wieczyście.

Prawa osób, których dane dotyczą.
Zgodnie z RODO przysługuje Państwu:
a) prawo dostępu do swoich danych oraz otrzymania ich kopii;
b) prawo do sprostowania (poprawiania) swoich danych;
c) prawo do usunięcia danych osobowych, w sytuacji, gdy przetwarzanie danych nie następuje w celu wywiązania się z obowiązku wynikającego z przepisu prawa lub w ramach sprawowania władzy publicznej;
d) prawo do ograniczenia przetwarzania danych;
e) prawo do wniesienia skargi do Prezesa UODO (na adres Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00 - 193 Warszawa)

Informacja o wymogu podania danych.
Podanie przez Państwa danych osobowych w niniejszym formularzu jest obowiązkiem wynikającym z art. 33 ust. 3 RODO oraz z art. 63 § 2-3a ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego.

[1] 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 (RODO) oraz podjętych działań.

[2] Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości

Załącznik nr 7
do Polityka Ochrony Danych Osobowych w spółce Centro-Chem Sp. z o.o. Sp.k.

OŚWIADCZENIE

Ja niżej podpisany(a) oświadczam, że zapoznałem/am się z ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych, rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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 „RODO"), a także Polityką Bezpieczeństwa, którego niniejsze Oświadczenie stanowi załącznik oraz Instrukcją Zarządzania Systemem Informatycznym, który stanowi załącznik do Polityki Bezpieczeństwa. Jednocześnie zobowiązuje się do zapewnienia ochrony przetwarzanych przez niego danych osobowych

……
(Miejsce i data złożenia oświadczenia)

……
(Numer PESEL)

…….

(Podpis osoby składającej oświadczenie)

Załącznik nr 8
do Polityka Ochrony Danych Osobowych w spółce Centro-Chem Sp. z o.o. Sp.k.

Turka, dnia ..... r.

UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) – dalej **RODO** − nadaję upoważnienie Pani/Panu:

……
(imię i nazwisko)

…….
(stanowisko)

do przetwarzania danych osobowych w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku, tj. uzyskuje Pani/Pan upoważnienie do przetwarzania danych osobowych w zakresie określonym przez Politykę ochrony danych osobowych.

Jednocześnie zobowiązuję Panią/Pana do przetwarzania danych osobowych, zgodnie z udzielonym upoważnieniem oraz z przepisami prawa powszechnie obowiązującego, a także z Polityką ochrony danych osobowych i załączonej do niej Polityką Bezpieczeństwa Informacji Systemów IT.

Jednocześnie upoważniam Panią/Pana do tworzenia/posiadania dla potrzeb wykonywanej pracy zestawień, ewidencji oraz rejestrów z danymi osobowymi, z zachowaniem pełnej ich ochrony przy zastosowaniu środków technicznych i organizacyjnych wdrożonych w Polityce ochrony danych osobowych Pracodawcy.

.....
podpis osoby uprawnionej do nadania upoważnienia

Upoważnienie odwołano w dniu ……..…..……..

.....
podpis osoby uprawnionej do odwołania upoważnienia

Niniejszym oświadczam, że zapoznałem/zapoznałam się z treścią Polityki ochrony danych osobowych, Ustawą, RODO oraz zakresem upoważnienia do przetwarzania danych osobowych określonym w Rejestrze Czynności Przetwarzania Danych Osobowych. Zobowiązuję się zachować w tajemnicy wszelkie informacje, które uzyskałem/uzyskałam w związku z przetwarzaniem danych osobowych, w tym informacje o zabezpieczeniach takiego przetwarzania.

.....
podpis osoby upoważnionej do przetwarzania

Załącznik nr 9
do Polityka Ochrony Danych Osobowych w spółce Centro-Chem Sp. z o.o. Sp.k.

(*miejscowość, data*)

Pani/Pan

Stanowisko: Inspektor Ochrony Danych

Podmiot:

(*nazwa Administratora Danych Osobowych*)

Wyznaczenie Inspektora Ochrony Danych[6]

Na podstawie z art. 37 ust. 1 lit. a, b, c, ust. 4 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz. UE L 2016, Nr 119, s. 1, dalej „RODO") wyznaczam, z dniem r., na stanowisko Inspektora Ochrony Danych Panią/Pana .

Podstawą współpracy jest: umowa o pracę/umowa cywilno-prawna/umowa o współpracy w zakresie świadczenia usług/* zawarta pomiędzy:

(*nazwa Administratora*)

a

(*firma/Partner kontraktu na świadczenie usług Inspektora Ochrony Danych*)

zwana dalej „Umową".

Upoważniam Panią/Pana do samodzielnego przebywania w strefie przetwarzania danych osobowych oraz do przetwarzania danych osobowych zgromadzonych przez w celu realizacji Umowy i wykonywania obowiązków

(*nazwa Administratora*)

Inspektora Ochrony Danych wynikających z art. 39 RODO oraz dodatkowo zleconych, na podstawie art. 38 ust. 6 RODO, zadań i obowiązków związanych z ochroną danych osobowych i bezpieczeństwem informacji:

1) ;

2) ;

[6] Wpisać właściwą nazwę.

3) .

Niniejszy dokument traci moc z chwilą: odwołania z funkcji Inspektora Ochrony Danych, cofnięcia upoważnienia lub rozwiązania Umowy.

W imieniu Administratora Danych Osobowych

Przyjmuję do wiadomości

(*podpis*)

Załącznik nr 10
do Polityka Ochrony Danych Osobowych w spółce Centro-Chem Sp. z o.o. Sp.k.

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH[7]

Zawarta w dniu ..... w ..... (zwana dalej umową) pomiędzy:
..... sp. z o.o. z siedzibą w ....., zarejestrowaną w rejestrze przedsiębiorców Krajowego Rejestru Sądowego prowadzonym przez Sąd Rejonowy w ..... Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS ....., NIP .....,
REGON .....,
reprezentowaną przez: .....,
zwaną dalej Administratorem[8],

---

[7] Powierzenie przetwarzania danych w imieniu administratora przez podmiot przetwarzający reguluje art. 28 RODO. Umowa, obok "innych instrumentów prawnych" podlegających prawu Unii lub innego państwa członkowskiego, które wiążą administratora i podmiot przetwarzający, jest wprost wymieniona w art. 28 ust. 3 RODO jako podstawa prawna przetwarzania przez podmiot przetwarzający danych osobowych. Przepis ten wskazuje również na wymagania dotyczące treści umowy, które obejmują konieczność określenia przedmiotu i czasu trwania przetwarzania; charakteru i celu przetwarzania; rodzaju danych osobowych oraz kategorii osób, których dane dotyczą, jak również obowiązków i praw administratora. Przedmiotem przetwarzania będą wszelkie operacje wykonywane na danych. Określenie celu i charakteru przetwarzania oraz rodzaju danych osobowych sprowadza się zaś do doprecyzowania, jakie kategorie danych i po co zostały powierzone do przetwarzania, a także w jaki sposób mają być przetwarzane.
Umowa powierzenia przetwarzania danych osobowych zazwyczaj ma charakter akcesoryjny. Celem jej zawarcia jest uregulowanie kwestii przekazania danych osobowych w związku z realizacją umowy zasadniczej dotyczącej przykładowo takich obszarów, jak finanse i rachunkowość, obsługa kadrowa, działania marketingowe, usługi IT. Zagadnienie powierzenia przetwarzania danych osobowych może zostać uregulowane zarówno w umowie zasadniczej, jak i zostać ujęte w osobnym dokumencie określanym właśnie mianem umowy powierzenia przetwarzania danych osobowych lub umowy o powierzenie przetwarzania danych osobowych.
Przepisy RODO przewidują możliwość zastosowania standardowych klauzul umownych w relacjach powierzenia. Klauzule te mogą być tworzone na szczeblu Komisji Europejskiej, co przewiduje art. 28 ust. 7 RODO, jak i mogą być wydawane przez organy nadzoru w procedurze spójności, jak wynika to z art. 28 ust. 8 RODO.
Umowa powierzenia przetwarzania danych osobowych zazwyczaj klasyfikowana jest jako umowa o świadczenie usług, do której odpowiednio stosuje się przepisy dotyczące umowy zlecenia (art. 750 k.c.).
Jak wynika to z art. 28 ust. 9 RODO, umowa o powierzenie przetwarzania danych osobowych wymaga formy pisemnej, w tym elektronicznej. Do zachowania wymaganej prawem formy wystarczające jest użycie formy, która odpowiadałaby zakresowi pojęcia formy dokumentowej (art. 77^2 k.c.).

[8] Stroną umowy o powierzenie przetwarzania danych jest administrator oraz podmiot przetwarzający dane, zwany także procesorem. Zarówno pojęcie administratora, jak i podmiotu przetwarzającego zostały zdefiniowane w RODO. Podkreślić należy, że rozporządzenie nie zrywa z dotychczasową siatką pojęć charakterystycznych dla prawa ochrony danych osobowych, jaki ukształtował się na gruncie dyrektywy 95/46/WE i uchylonej ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych.
Zgodnie z treścią art. 4 pkt 7 RODO administratorem jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Administratorem może być zarówno podmiot sektora prywatnego, działający w różnych formach prawnych (np. spółki kapitałowe, spółdzielnie, fundacje, stowarzyszenia), jak i podmioty należące do sektora publicznego.
Status administratora danych nie wynika z samego faktu posiadania danych, ale ze sprawowania faktycznej kontroli nad ich przetwarzaniem, obejmującej dwa elementy, a mianowicie decydowanie o celach i środkach przetwarzania danych. Jeśli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są

a

..... sp. z o.o. z siedzibą w ....., zarejestrowaną w rejestrze przedsiębiorców Krajowego Rejestru Sądowego prowadzonym przez Sąd Rejonowy w ..... Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS ....., NIP ....., REGON .....,

reprezentowaną przez: .....,

zwanym dalej Podmiotem przetwarzającym[9],

zwanymi łącznie w dalszej części umowy Stronami, a każda z osobna Stroną.

Zważywszy, że

1. Strony zawarły umowę ..... (zwana dalej umową podstawową), w związku z wykonaniem której Administrator powierzy Podmiotowi przetwarzającemu przetwarzanie danych osobowych w zakresie określonym niniejszą umową.
2. Celem umowy jest ustalenie warunków, na jakich Podmiot przetwarzający wykonuje operacje przetwarzania danych osobowych w imieniu Administratora.
3. Strony dążą do takiego uregulowania zasad przetwarzania danych osobowych, aby odpowiadały one w pełni postanowieniom rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679

---

oni współadministratorami (art. 26 ust. 1 RODO). W takiej sytuacji pozycję administratora jako strony umowy zajmować może więcej niż jeden podmiot prawa.
W przypadku powierzenia przetwarzania danych administrator nadal decyduje o celu i sposobie przetwarzania danych i ponosi odpowiedzialność za spełnienie wymogów określonych przepisami prawa. Na administratorze danych spoczywa odpowiedzialność za zawarcie umowy powierzenia przetwarzania danych, a także obowiązek korzystania w tym zakresie z usług podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą, w szczególności, jeśli chodzi o wiedzę fachową, wiarygodność i zasoby (art. 28 ust. 1 RODO). Jako dobrą praktykę wykazującą dochowanie należytej staranności przez administratora w tym zakresie można wskazać na przykład wystosowanie pytań dotyczących ochrony danych osobowych do podmiotu przetwarzającego czy też przeprowadzenie audytu bezpieczeństwa u przyszłego kontrahenta. Dodatkowa weryfikacja nie jest konieczna, jeśli podmiot przetwarzający stosuje zatwierdzony kodeks postępowania (art. 40 RODO) lub zatwierdzony mechanizm certyfikacji (art. 42 RODO). Przyjmuje się wówczas, że spełnia on wymogi, o których mowa w art. 28 ust. 1 RODO.

[9] Pojęcie podmiotu przetwarzającego – zgodnie z art. 4 pkt 8 RODO – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora. Status podmiotu przetwarzającego dane uzyskuje podmiot, prawnie odrębny od administratora, działający w jego imieniu, który faktycznie, a nie jedynie formalnie, bierze udział w zleconej przez administratora operacji przetwarzania danych. Podmiotem przetwarzającym dane może być między innymi dostawca usługi w chmurze obliczeniowej, podmiot świadczący usługi reklamowe lub marketingowe, biura rachunkowe, przedsiębiorcy świadczący usługi kurierskie czy usługę archiwizacji i brakowania dokumentów, centra telefoniczne. Dla kwalifikacji podmiotu jako przetwarzającego dane bez znaczenia pozostaje forma prawna, w jakiej działa. Podmiotem przetwarzającym może być zarówno podmiot prywatny (osoba fizyczna, osoba prawna, jednostka organizacyjna mająca zdolność prawną, ale nieposiadająca osobowości prawnej), jak i publiczny (organ administracji publicznej, inny podmiot publiczny). Wybór podmiotu przetwarzającego zależy od decyzji podjętej przez administratora danych, który może zdecydować o przetwarzaniu danych w ramach własnej struktury organizacyjnej, na przykład przez pracowników upoważnionych do przetwarzania danych pod jego bezpośrednim zwierzchnictwem, lub przekazać całość bądź część działań w zakresie przetwarzania danych odrębnemu podmiotowi, działającemu w imieniu administratora.
Zgodnie z art. 29 RODO podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego. Zatem podmiot przetwarzający działa na zlecenie administratora i może przetwarzać dane w zakresie i w sposób przez administratora wskazany, nie może w tym zakresie decydować samodzielnie.

z 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 (dalej: RODO) (Dz. Urz. UE L 119 z 4.05.2016 r., s. 1).

4. Administrator oświadcza, że jest uprawniony do przetwarzania danych, które powierza Podmiotowi przetwarzającemu w celu realizacji umowy podstawowej oraz że jest uprawniony do ich przetwarzania, w zakresie, w jakim powierzył je Podmiotowi przetwarzającemu.
5. Podmiot przetwarzający oświadcza, że dysponuje odpowiednimi środkami technicznymi i organizacyjnymi, by przetwarzanie powierzonych danych osobowych było zgodne z aktualnymi przepisami o ochronie danych osobowych i chroniło prawa osób, których dane dotyczą. Formularz oceny podmiotu przetwarzającego zawiera załącznik nr 1 do umowy.

Strony zgodnie postanowiły, co następuje.

§ 1

Przedmiot umowy

1. W związku z zawarciem umowy podstawowej Administrator powierza Podmiotowi przetwarzającemu przetwarzanie danych osobowych wskazanych w § 2 umowy (dalej: dane osobowe)[10].
2. Podmiot przetwarzający będzie przetwarzał powierzone przez Administratora dane osobowe wyłącznie w celu realizacji umowy podstawowej, tj. ..... (*należy określić cel przetwarzania danych przez podmiot przetwarzający wynikający z umowy podstawowej*).
3. Podmiot przetwarzający jest uprawniony do wykonywania, w sposób zautomatyzowany oraz niezautomatyzowany, operacji przetwarzania danych osobowych, takich jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

§ 2

[10] Istotą powierzania przetwarzania danych osobowych jest zlecenie przez administratora podmiotowi przetwarzającemu dokonania określonych czynności przetwarzania. RODO definiuje przetwarzanie jako operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie przez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie (art. 4 pkt 2 RODO). Katalog działań wymienianych w przepisach prawa jako czynności przetwarzania ma charakter otwarty. Wskazując w umowie operacje, jakich dokonywać będzie podmiot przetwarzający, zarówno zautomatyzowane, jak i niezautomatyzowane, wskazać należy te, które faktycznie będą wykonywane.

Dane osobowe

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie niniejszej umowy, następujące rodzaje danych osobowych[11]:
   Dane zwykłe:
   1) imię,
   2) nazwisko,
   3) numer ewidencyjny PESEL,
   4) adres e-mail,
   5) .....
2. Przetwarzanie danych będzie dotyczyć następujących kategorii osób:
   1) klienci Administratora;
   2) .....

§ 3

Obowiązki Podmiotu przetwarzającego[12]

[11] Zgodnie z wynikającym z art. 28 ust. 3 RODO wymogiem w umowie należy wskazać rodzaj danych osobowych przetwarzanych przez podmiot przetwarzający w imieniu administratora. Definicję pojęcia danych osobowych, które są przedmiotem świadczenia umowy, zawiera art. 4 pkt 1 RODO. Danymi osobowymi – w rozumieniu art. 4 pkt 1 RODO – są wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"). Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie takiego identyfikatora, jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Pojęcie danych osobowych ma szeroki zakres przedmiotowy i obejmuje różnego rodzaju informacje, które dotyczą konkretnej osoby fizycznej. Daną osobową, oprócz imienia i nazwiska, może być numer Powszechnego Elektronicznego Systemu Ewidencji Ludności – PESEL, numer identyfikacji podatkowej – NIP, wizerunek lub też adresy e-mail, numer IP czy identyfikatorów plików cookie, o ile umożliwiają identyfikację osoby fizycznej. Określony przez strony zakres powierzonych danych musi obejmować dane, do przetwarzania których upoważniony jest administrator.
Opisując zakres przetwarzanych danych, określić należy również kategorię danych osobowych. Mianowicie należy wskazać, czy powierzone dane należą do kategorii tzw. danych zwykłych, czy powierzenie obejmuje także dane o szczególnym charakterze, o których mowa w art. 9 i 10 RODO. Przepisy te regulują odpowiednio kwestie przetwarzania danych sensytywnych (np. dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne), a także dane dotyczące wyroków skazujących i naruszeń prawa.
W umowie należy wskazać również kategorie osób, których dane będą przetwarzane w związku z realizacją umowy podstawowej. Kategorie osób, których dane dotyczą, obejmują różnego rodzaju osoby fizyczne, których dane osobowe są przetwarzane. Kategorie te mogą obejmować na przykład dzieci i przedstawicieli innych grup szczególnie wrażliwych, pracowników i współpracowników administratora czy też jego klientów.
[12] Istotne dla sformułowania obowiązków ciążących na podmiocie przetwarzającym są postanowienia art. 28 ust. 3 RODO. Przepis ten wskazuje na wiele obowiązków spoczywających na tym podmiocie, jak: wymóg przetwarzania danych osobowych na wyłączne udokumentowane polecenie administratora (art. 28 ust. 3 lit. a RODO), zapewnienia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy (art. 28 ust. 3 lit. a RODO), wymóg podejmowania wszelkich środków zapewniających bezpieczeństwo danych osobowych wymaganych na mocy art. 32 RODO, przestrzeganie warunków korzystania z usług innego podmiotu przetwarzającego (podprzetwarzającego), obowiązek pomocy administratorowi poprzez odpowiednie środki techniczne i organizacyjne w wywiązaniu się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO czy pomoc administratorowi w wywiązaniu się z obowiązków określonych w art. 32–36 RODO, a także obowiązek usunięcia lub zwrotu wszelkich danych osobowych i ich kopii po zakończeniu umowy (art. 28 ust. 3 lit. g RODO), jak również udostępniania administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków, oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich. Do obowiązków podmiotu przetwarzającego zaliczyć należy także prowadzenie rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu

1. Podmiot przetwarzający zobowiązuje się do przetwarzania danych wyłącznie w celu, dla którego zostały one powierzone.
2. Podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora, chyba że obowiązek przetwarzania danych osobowych wynika z przepisów prawa, w takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podmiot przetwarzający ma obowiązek niezwłocznie informować Administratora, jeżeli jego zdaniem polecenie Administratora jest niezgodne z prawem.
4. Podmiot przetwarzający zobowiązuje się nie przekazywać danych osobowych do państwa trzeciego lub organizacji międzynarodowej ani nie korzysta z usług innych podmiotów przetwarzających, które przekazują dane osobowe do państwa trzeciego lub organizacji międzynarodowej.
5. Podmiot przetwarzający zobowiązuje się do wdrożenia odpowiednich środków technicznych i organizacyjnych zmierzających do zapewnienia bezpieczeństwa przetwarzania, tak aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych. Środki techniczne i organizacyjne stosowane przez Podmiot przetwarzający zostały opisane w załączniku nr 2 do umowy[13].

---

administratora, o którym mowa w art. 30 ust. 2 RODO, czy obowiązku zgłaszania bez zbędnej zwłoki administratorowi przypadków naruszenia ochrony danych osobowych, o czym stanowi art. 33 RODO.

[13] Przepis art. 28 ust. 3 lit. c RODO wskazuje jako element umowy z podmiotem przetwarzającym także aspekty dotyczące środków zapewniających bezpieczeństwo przetwarzania zgodnie z art. 32 RODO. Stosownie zaś do treści art. 32 ust. 1 lit. b RODO, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania, jak i ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku pseudonimizację i szyfrowanie danych osobowych, zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego oraz regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania. W myśl art. 32 ust. 2 RODO, oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Stosownie do art. 32 ust. 3 RODO wywiązywanie się z tak określonych obowiązków można wykazać między innymi przez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 RODO, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42 RODO.
Celem regulacji zawartej w art. 32 RODO jest zobowiązanie administratora oraz podmiotu przetwarzającego do wdrożenia rozwiązań technicznych i organizacyjnych mających zapewnić bezpieczeństwo nie tylko danych, lecz także operacji ich przetwarzania.
Środki zabezpieczenia prawodawca unijny podzielił na dwie grupy: środki techniczne i środki organizacyjne. Przepisy rozporządzenia nie wskazują jednak konkretnych środków technicznych lub organizacyjnych, które należy zastosować, aby wykazać zgodność z określonymi w nim wymaganiami. Wybór środków bezpieczeństwa powinien być determinowany przez okoliczności i warunki przetwarzania danych oraz prawdopodobieństwo i powagę zdarzeń, które mogą doprowadzić do naruszenia praw i wolności osób, których dane są przetwarzane. Środki te powinny być odpowiednie, przez co rozumieć należy dążenie do tego, aby środki były skuteczne, a więc pozwalały na zapobieganie naruszeniom ochrony danych lub ograniczenie do minimum ryzyka ich wystąpienia.

6. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych każdej osobie fizycznej, która będzie przetwarzała powierzone dane osobowe, przy czym będą to jedynie osoby, które posiadają odpowiednie przeszkolenie z zakresu ochrony danych osobowych.
7. Podmiot przetwarzający zobowiązuje się zapewnić, aby każda osoba fizyczna, która ma dostęp do danych osobowych z upoważnienia Podmiotu przetwarzającego, zobowiązała się do zachowania ich w tajemnicy.
8. Podmiot przetwarzający zobowiązuje się do prowadzenia dokumentacji opisującej sposób przetwarzania danych osobowych, w tym do prowadzenia rejestru kategorii czynności przetwarzania danych osobowych dokonywanych w imieniu Administratora, w przypadku obowiązku prowadzenia takiego rejestru.
9. Podmiot przetwarzający oświadcza, że wyznaczył Inspektora Ochrony Danych w osobie: .....
10. Podmiot przetwarzający zobowiązuje się do współpracy z Administratorem, przy uwzględnieniu charakteru przetwarzania, w wywiązaniu się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej prawa do uzyskania informacji, prawa dostępu do danych, prawa do sprostowania danych, usunięcia danych, ograniczenia przetwarzania danych, przenoszenia danych oraz prawa sprzeciwu, poprzez odpowiednie środki techniczne i organizacyjne. W razie wpływu takiego żądania Podmiot przetwarzający niezwłocznie przekazuje je Administratorowi pocztą elektroniczną na adres: ....., nie później jednak niż w terminie trzech dni od otrzymania żądania.
11. Podmiot przetwarzający zobowiązuje się do współpracy z Administratorem w zakresie realizacji obowiązków określonych w art. 32–36 RODO, tj. zabezpieczenia danych, zgłaszania naruszenia ochrony danych, zawiadamiania osób, których dane dotyczą, o naruszeniu, dokonywania oceny skutków dla ochrony danych oraz uprzednich konsultacji z organem nadzorczym w zakresie powierzonych danych.
12. Podmiot przetwarzający zobowiązuje się niezwłocznie, nie później jednak niż w terminie 24 godzin, informować Administratora o wszelkich stwierdzonych naruszeniach danych osobowych pocztą elektroniczną na adres ..... [14].

Mogą to być między innymi takie środki, jak: zamki w drzwiach, systemy alarmowe, zabezpieczenie dostępu hasłem w systemie informatycznym, szyfrowanie danych zawartych na dysku czy wyodrębnienie stref ograniczonego dostępu itp. W umowie można zawrzeć klauzulę odsyłającą w zakresie opisu środków technicznych i organizacyjnych, stosowanych przez podmiot przetwarzający, do odpowiedniego załącznika lub zamieścić ich opis lub listę bezpośrednio w tekście głównym umowy.

[14] Termin „naruszenie ochrony danych osobowych" został zdefiniowany w art. 4 pkt 12 RODO jako naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych (np. poprzez utratę lub kradzież urządzenia, na którym przechowywana jest kopia bazy danych klientów administratora). Zgodnie z przepisami RODO administratorzy zobowiązani są do zgłaszania naruszeń, chyba że dane naruszenie najprawdopodobniej nie będzie wiązało się z

§ 4

Obowiązki Administratora

1. Administrator zobowiązuje się współdziałać z Podmiotem przetwarzającym w wykonaniu umowy, w tym do udzielenia Podmiotowi przetwarzającemu wszelkich informacji, niezbędnych do wykonania umowy.
2. Administrator zobowiązuje się dokumentować w formie pisemnej wszystkie polecenia dotyczące przetwarzania danych osobowych dla Podmiotu przetwarzającego.
3. Administrator zobowiązuje się do przekazania informacji osobom, których dane dotyczą, o operacjach przetwarzania w momencie zebrania danych.

§ 5

Kontrola

1. Na wniosek Administratora, Podmiot przetwarzający udostępnia wszelkie informacje niezbędne do realizacji lub wykazania spełnienia obowiązków wynikających z RODO.
2. Administrator zastrzega sobie prawo do przeprowadzenia kontroli wykonywania umowy, nie rzadziej niż co 12 miesięcy oraz zawsze w przypadku stwierdzenia naruszenia ochrony danych osobowych przez Podmiot przetwarzający. Podmiot przetwarzający zobowiązuje się do należytego współdziałania z Administratorem w czynnościach kontrolnych. W szczególności Podmiot przetwarzający zobowiązany jest do:
    1) udostępnienia Administratorowi dokumentacji przetwarzania danych osobowych;
    2) udostępnienia Administratorowi dostępu do pomieszczeń, w których przetwarzane są dane osobowe;
    3) umożliwienia Administratorowi sporządzania kopii dokumentów dotyczących przetwarzania danych osobowych[15].

ryzykiem naruszenia praw i wolności osób fizycznych. Podmioty przetwarzające muszą zaś zgłaszać wszelkie naruszenia administratorowi. W art. 33 ust. 2 RODO wskazano wyraźnie, że w przypadku, gdy administrator korzysta z usług podmiotu przetwarzającego, a podmiot przetwarzający stwierdzi wystąpienie naruszenia ochrony danych osobowych, które przetwarza w imieniu administratora, musi zgłosić to naruszenie administratorowi "bez zbędnej zwłoki". Zaleca się, aby podmiot przetwarzający szybko zgłaszał naruszenia administratorowi i następnie stopniowo przekazywał dalsze informacje na temat naruszenia, w miarę uzyskiwania dostępu do bardziej szczegółowych danych. Ma to istotne znaczenie dla ułatwienia administratorowi spełnienia wymogu zgłoszenia naruszenia właściwemu organowi nadzorczemu, tj. Prezesowi Urzędu Ochrony Danych Osobowych, w terminie 72 godzin, zgodnie z art. 33 ust. 1 RODO, oraz zawiadomić o jego wystąpieniu osoby fizyczne, na które naruszenie wywiera wpływ, zgodnie z art. 34 ust. 1 RODO.
Wskazać należy, jak wynika z art. 32 RODO, że administrator i podmiot przetwarzający powinni dysponować odpowiednimi środkami technicznymi i organizacyjnymi, aby zapewnić odpowiedni stopień bezpieczeństwa danych osobowych. Zdolność do wykrywania naruszeń, zaradzania im oraz ich terminowego zgłaszania powinna być postrzegana jako najważniejszy element tych środków.

[15] Istotne jest, aby administrator danych, powierzający w trybie art. 28 RODO dane osobowe innemu podmiotowi, zachował możliwość kontroli nad tym, czy podmiot, któremu dane powierzono, przetwarza je zgodnie z przepisami prawa i postanowieniami łączącej strony umowy powierzenia przetwarzania danych. Zgodnie z art. 28 ust. 3 lit. h RODO umowa stanowi w szczególności, że podmiot przetwarzający udostępnia administratorowi

3. Kontrola będzie przeprowadzona po uprzednim zawiadomieniu Podmiotu przetwarzającego o terminie kontroli. Kontrola przeprowadzona będzie w godzinach pracy Podmiotu przetwarzającego.
4. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli i wdrożenia zaleceń Administratora w terminie nie dłuższym niż 10 dni. Podmiot przetwarzający niezwłocznie przekaże Administratorowi informacje o podjętych działaniach.
5. Uprawnienia określone w § 5 pkt 1–2 umowy przysługują Administratorowi odpowiednio w stosunku do podmiotów, którym Podmiot przetwarzający powierzył dalsze przetwarzanie danych osobowych zgodnie z § 6 pkt 1 umowy.
6. Administrator zastrzega sobie prawo korzystania z usług osób trzecich celem przeprowadzenia kontroli (audytorów), jak również do przeprowadzenia takiej kontroli samodzielnie.
7. Podmiot przetwarzający przed podpisaniem umowy zobowiązuje się udzielić informacji dotyczących zabezpieczeń technicznych i organizacyjnych dotyczących powierzonych przez Administratora danych osobowych, celem weryfikacji rękojmi bezpiecznego i zgodnego z prawem przetwarzania danych osobowych.

§ 6

Podpowierzenie

1. Podmiot przetwarzający może powierzyć konkretne operacje na danych osobowych do dalszego przetwarzania w drodze pisemnej umowy zawartej z innym podmiotem przetwarzającym, wyłącznie po uzyskaniu uprzedniej pisemnej zgody Administratora[16].

wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich. Ponadto podmiot przetwarzający niezwłocznie informuje administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie rozporządzenia lub innych przepisów Unii lub państwa członkowskiego o ochronie danych.

[16] W umowie powierzenia przetwarzania danych należy także uregulować zagadnienie dalszego powierzenia przetwarzania danych osobowych podmiotowi trzeciemu, tzw. dalszego powierzenia lub podpowierzenia. Z sytuacją taką mamy do czynienia, gdy podmiot, któremu administrator powierzył przetwarzanie danych, zleca innemu podmiotowi wykonanie określonych czynności przetwarzania danych. Do kwestii podpowierzenia przetwarzania danych odnosi się art. 28 ust. 2 RODO, zgodnie z którym podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian. Oznacza to, że podmiot przetwarzający może dokonać podpowierzenia jedynie po uzyskaniu zgody administratora: ogólnej bądź szczegółowej, odnoszącej się do konkretnego podmiotu trzeciego. W przypadku udzielenia przez administratora zgody ogólnej, podmiot przetwarzający ma obowiązek informować o wszelkich zamierzonych zmianach w tym zakresie. Zmiany dotyczyć mogą zarówno decyzji podmiotu przetwarzającego o zamiarze podpowierzenia danych kolejnemu podmiotowi trzeciemu, jak i zastąpienia zaakceptowanego podmiotu trzeciego innym podmiotem. Administrator w każdym przypadku zachowuje możliwość wyrażenia sprzeciwu wobec zmian zaproponowanych przez podmiot przetwarzający.
Jednocześnie zgodnie z art. 28 ust. 4 RODO, jeżeli do wykonania w imieniu administratora konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot

2. Podmiot przetwarzający zobowiązuje się zapewnić, aby podmiot, któremu powierzono dalsze przetwarzanie danych osobowych zgodnie z § 6 pkt 1 umowy, spełniał co najmniej te same gwarancje i wymagania dotyczące ochrony danych osobowych, jakie zostały nałożone na Podmiot przetwarzający na mocy umowy. W szczególności wymóg ten dotyczy obowiązku zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom RODO.
3. Podmiot przetwarzający ma obowiązek niezwłocznie informować Administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających. Administrator ma prawo wyrazić sprzeciw wobec zamierzonych przez podmiot przetwarzający zmian.
4. Podmiot przetwarzający nie może powierzyć innemu podmiotowi przetwarzającemu całości wykonania umowy.
5. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na podwykonawcy obowiązków wynikających z umowy.

§ 7

Wynagrodzenie

Wynagrodzenie należne Podmiotowi przetwarzającemu na podstawie umowy podstawowej obejmuje wynagrodzenie należne z tytułu umowy.

§ 8

Czas

1. Umowa zostaje zawarta na czas obowiązywania umowy podstawowej[17].

przetwarzający nałożone zostają – na mocy umowy – te same obowiązki ochrony danych jak w umowie między administratorem a podmiotem przetwarzającym.
Przepis ten odnosi się do obowiązków wynikających z art. 28 ust. 3 RODO, w tym w szczególności do obowiązku zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom RODO.

Pełna odpowiedzialność wobec administratora za wypełnienie obowiązków przez podprzetwarzającego spoczywa na pierwotnym podmiocie przetwarzającym. Oznacza to, że kontrola administratora nad łańcuchem powierzenia, jaki tworzy się w związku z dalszym podpowierzaniem danych podmiotom trzecim, ograniczona jest do pierwszego ogniwa, tj. podmiotu przetwarzającego.

[17] Jak stanowi art. 28 ust. 3 RODO, umowa, na podstawie której odbywa się przetwarzanie danych osobowych przez podmiot przetwarzający, powinna określać między innymi czas trwania przetwarzania. Regulacja ta koresponduje z ogólną zasadą ograniczonego przechowywania, sformułowaną w art. 5 ust. 1 lit. e RODO, w myśl której dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.
Po zakończeniu przetwarzania w imieniu administratora podmiot przetwarzający powinien – zgodnie z decyzją administratora – zwrócić lub usunąć dane osobowe, chyba że prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający, nakładają obowiązek przechowywania danych osobowych (motyw 81 RODO). Administrator ma prawo decydować, czy po zakończeniu umowy podmiot przetwarzający powinien powierzone mu dane usunąć czy też zwrócić.

2. Z chwilą zakończenia obowiązywania umowy podstawowej Podmiot przetwarzający zobowiązuje się w zależności od żądania Administratora zwrócić lub usunąć powierzone dane Administratorowi oraz usunąć wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazuje przechowywanie danych osobowych.

§ 9

Postanowienia końcowe

1. Wszelkie zmiany i uzupełnienia postanowień niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.
2. W sprawach nieuregulowanych w niniejszej umowie zastosowanie mają przepisy kodeksu cywilnego, RODO, a także przepisy innych ustaw regulujących ochronę danych osobowych.
3. Wszelkie spory mogące wyniknąć w związku z zawarciem lub wykonaniem umowy rozstrzygane będą przez sąd miejscowo właściwy dla siedziby Administratora.
4. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
5. Umowa wchodzi w życie z dniem podpisania.

....

Administrator Podmiot przetwarzający

Załączniki:

1) załącznik nr 1 – formularz oceny podmiotu przetwarzającego, wypełniony przez Podmiot przetwarzający przed podpisaniem umowy podstawowej
2) załącznik nr 2 – wykaz środków technicznych i organizacyjnych stosowanych przez Podmiot przetwarzający

Załącznik nr 12
do Polityka Ochrony Danych Osobowych w spółce Centro-Chem Sp. z o.o. Sp.k.

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

Lp.	Dokładny adres	Dział użytkujący pomieszczenie	Nr pokoju lub pomieszczenia	Rodzaj zastosowanego zabezpieczenia pomieszczenia	Uwagi

……
Data i podpis Administratora

Załącznik nr 13
do Polityka Ochrony Danych Osobowych w spółce Centro-Chem Sp. z o.o. Sp.k.

KLAUZULA INFORMACYJNA O PRZETWARZANIU DANYCH OSOBOWYCH
dla kandydatów do pracy w Centro-Chem Sp. z o.o. Sp.k.

Stosownie do postanowień art. 13 ust. 1 i ust. 2 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 realizujemy obowiązek informacyjny.

1. **Informacje o Administratorze Danych Osobowych i Inspektorze Ochrony Danych**

Administratorem Danych Osobowych jest **Spółkę Centro-Chem spółka z ograniczoną odpowiedzialnością spółka komandytowa, Turka 141B, 20-258 Lublin**, e-mail: info@centro-chem.pl, tel. 81 756 55 20.

W sprawie gromadzenia, przetwarzania i ochrony danych można kontaktować się z Inspektorem Danych Osobowych pod adresem: Centro-Chem spółka z ograniczoną odpowiedzialnością spółka komandytowa, Turka 141B, 20-258 Lublin, e-mail: iod@centro-chem.pl.

2. **Informacje o pobieranych/gromadzonych danych:**
    1) Cel przetwarzania: przeprowadzenie naboru , w tym nawiązanie kontaktu na etapie prowadzenia tego procesu oraz nawiązanie stosunku pracy w przypadku pozytywnego jej zakończenia, a także archiwizacja dokumentów po przeprowadzeniu naboru zgodnie z wymogami prawa powszechnie obowiązującego.
    2) Podstawą przetwarzania danych osobowych jest: ,
        a) art. 6 ust. 1 lit. b RODO,
        b) art. 6 ust. 1 lit. c RODO w zw. z art. 22^1 Kodeksu pracy oraz ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach,
        c) art. 6 ust. 1 lit. a RODO oraz art. 9 ust. 2 lit. a RODO.

Informacje dodatkowe o wymogu podania danych: Podanie danych osobowych w zakresie wynikającym z art. 22(1) Kodeksu pracy (m.in. imię, nazwisko, dane kontaktowe, wykształcenie, przebieg dotychczasowego zatrudnienia, wymagania do zatrudnienia) jest dobrowolne, jednak niezbędne, aby uczestniczyć w procesie naboru. Podanie innych danych w zakresie nieokreślonym przepisami prawa, zostanie potraktowane jako zgoda na przetwarzanie danych osobowych. Wyrażenie zgody w tym przypadku jest dobrowolne, a zgodę tak wyrażoną można odwołać w dowolnym czasie. Jeżeli podane dane będą obejmowały szczególne kategorie danych, o których mowa w art. 9 ust. 1 RODO[18], konieczna będzie wyraźna zgoda na ich przetwarzanie,

[18] Art. 9 RODO
ust. 1 - Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby;
ust. 2 - Ust. 1 nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków:
a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1;
b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem

która może zostać odwołana w dowolnym czasie. Zgodę należy w takim przypadku przekazać do Administratora wraz z dokumentami aplikacyjnymi. Proponowana treść zgody na przetwarzanie danych osobowych: „*Wyrażam zgodę na przetwarzanie moich danych osobowych wskazanych w art. 9 ust 1 RODO na potrzeby naboru prowadzonego przez Centro-Chem spółka z ograniczoną odpowiedzialnością spółka komandytowa i ewentualnie zawarcia umowo pracę zgodnie z wymogami RODO*";

3) Informacje o odbiorcach danych osobowych lub o kategoriach odbiorców - uprawnione na mocy prawa organy publiczne oraz podmioty świadczące usługi na rzecz Administratora, m.in. w zakresie:
    a) realizacji usługi niszczenia i archiwizacji dokumentacji,
    b) realizacji usług zaopatrujących Centro-Chem spółka z ograniczoną odpowiedzialnością spółka komandytowa w rozwiązania techniczne oraz organizacyjne zapewniające sprawne zarządzanie (w szczególności dostawcom usług teleinformatycznych, dostawcom sprzętu, firmom kurierskim i pocztowym, podmioty współpracujące przy opracowaniu wydawnictw i ich dystrybucji, podmioty obsługujące media społecznościowe);
    c) realizacji obsługi prawnej, ubezpieczeniowej, konsultingowej.
4) **Informacje o zamiarze przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji** międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO: Administrator Danych Osobowych korzysta z Microsoft 365, co może spowodować przekazanie Państwa danych osobowych do państwa trzeciego. Regulamin korzystania z Usług Microsoft w zakresie Microsoft 365 oraz zobowiązania w odniesieniu do przetwarzania i zabezpieczania danych użytkownika oraz danych osobowych przez usługi online określa dokumentacja Microsoft.

W ramach usług Microsoft, dane wprowadzone do Microsoft 365 będą przetwarzane i przechowywane w określonej lokalizacji geograficznej. Zgodnie z funkcjonalnością usług Microsoft w dostępnym panelu administracyjnym w „Profilu Organizacji", wskazano, iż dane przetwarzane są na terenie Unii Europejskiej.

Microsoft zobowiązuje się do przestrzegania przepisów prawa dotyczących świadczenia Usług Online, które dotyczą ogółu dostawców informatycznych. Microsoft realizuje coroczne audyty Usług Online, obejmujące audyty zabezpieczeń komputerów, środowiska informatycznego i fizycznych Centrów Danych, nadzorowany i upoważnione przez niego firmy trzecie, łącznie z prawem.

5) **Okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu:**
    a) dane osobowe są przetwarzane przez okres prowadzenia naboru,
    b) dokumenty aplikacyjne są niszczone w terminie 3 lat od dnia zakończenia procesu naboru (złożone dokumenty są usuwane z portalu, na którym zamieszczono ogłoszenie o naborze, elektronicznych skrzynek pocztowych, wydruki są niszczone); ze zniszczenia ww. dokumentów sporządzany będzie protokół, w którym będą wskazani kandydaci ubiegający się o pracę (imię i nazwisko oraz miejsce zamieszkania) na dane stanowisko, data zniszczenia dokumentów i podpisy osób uczestniczących w zniszczeniu dokumentów; ww.

zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;

dane osobowe będą przetwarzane wyłącznie w celu dowodowym i w celu rozliczalności przetwarzania danych osobowych;

c) dokumenty aplikacyjne zatrudnionej w wyniku naboru będą niszczone w terminie 1 roku od dnia ustania stosunku pracy, a w przypadku zgłoszenia roszczeń związanych ze stosunkiem pracy do czasu ich rozstrzygnięcia;
d) dokumenty aplikacyjne związane z naborem, przekazane po wyznaczonym w ogłoszeniu o naborze terminie składania aplikacji, nie będą rozpatrywane; będą one usuwane na zasadach określonych w lit. b;
e) dokumenty (w tym ewidencję osób uczestniczących w danym procesie naboru, która zawiera następujące dane osobowe: imię i nazwisko kandydata, adres e-mail, numer telefonu, miejsce zamieszkania) związane z naborem, z wyjątkiem dokumentów aplikacyjnych kandydatów, przechowywane są przez okres 2 lat.

6) **Informacja o profilowaniu** (przez profilowanie rozumie się dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się): nie są wykonywane takie operacje.

3. Informacja o prawach osoby, której dane są przetwarzane:

1) Posiada Pani/Pan prawo:
   a) dostępu do swoich danych osobowych,
   b) sprostowania swoich danych osobowych,
   c) usunięcia swoich danych osobowych,
   d) ograniczenia przetwarzania swoich danych osobowych,
   e) cofnięcia zgody na przetwarzanie danych osobowych poprzez złożenie/przesłanie pisma na adres: Centro-Chem spółka z ograniczoną odpowiedzialnością spółka komandytowa, Turka 141B, 20-258 Lublin, e-mail: iod@centro-chem.pl – jeżeli uprzednio wyrazili Państwo taką zgodę i przetwarzanie dotyczących Państwa danych odbywa się na jej podstawie,
   f) przenoszenia swoich danych osobowych,
   g) wniesienia sprzeciwu wobec przetwarzania swoich danych osobowych z przyczyn związanych z szczególną Państwa sytuacją zgodnie z art. 21 RODO.
2) Osobie, której dane są przetwarzane przysługuje prawo do złożenia skargi związanej z przetwarzaniem jej danych osobowych przez Administratora Danych Osobowych lub podmiot/organizację, której dane osobowe zostały przekazane do: Prezes Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa, tel. 22 531 03 00, https://uodo.gov.pl/p/kontakt.

Informujemy, że nasza siedziba objęta jest monitoringiem wizyjnym.

Informujemy, że użyte w niniejszej klauzuli informacyjnej skróty oznaczają:

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

2. **Odbiorca danych** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem powszechnie obowiązującym, nie są jednak uznawane za odbiorców - przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania; przy czym przez sformułowanie, „strona trzecia" rozumie się osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia Administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe.
3. **Przetwarzanie** - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
4. **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;
5. **Zgoda osoby, której dane dotyczą** – oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

Załącznik nr 4
do Polityka Ochrony Danych Osobowych w spółce Centro-Chem Sp. z o.o. Sp.k.

Polityka Bezpieczeństwa Informacji Systemów IT.

w wersji word