# Wiążące Reguły Korporacyjne obowiązujące w Grupie Roust

*Wersja: 1.0*

*Data: 25 maja 2018 r.*

## Spis treści

## 1. Wprowadzenie

1. Celem Wiążących Reguł Korporacyjnych („WRK") jest zapewnienie odpowiedniej ochrony w zakresie przekazywania i przetwarzania Danych Osobowych przez Roust Corporation i jej podmioty powiązane zaangażowane we wspólne działania gospodarcze („Grupa Roust").

2. Wszystkie spółki należące do Grupy Roust potwierdzają swoje zobowiązanie do zapewnienia zgodności z WRK.

3. WRK zobowiązują wszystkie spółki Grupy Roust oraz wszystkich pracowników Grupy Roust do przestrzegania określonych w nich zasad.

## 2. Definicje

W odniesieniu do WRK obowiązują następujące definicje:

1. „Dane Osobowe" oznaczają wszelkie informacje dotyczące zidentyfikowanych lub możliwych do zidentyfikowania osób;

   UWAGA: możliwa do zidentyfikowania osoba fizyczna to osoba, która może zostać zidentyfikowana bezpośrednio lub pośrednio, zwłaszcza na podstawie identyfikatora, takiego jak nazwisko, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator online, albo poprzez odniesienie do jednego lub większej liczby czynników dotyczących charakterystyki fizycznej, fizjologicznej, genetycznej, psychicznej, ekonomicznej, kulturalnej lub społecznej danej osoby fizycznej.

2. „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;

3. „Administrator" oznacza podmiot określający cele i sposoby przetwarzania Danych Osobowych;

4. „Podmiot Przetwarzający" oznacza podmiot przetwarzający Dane Osobowe w imieniu Administratora;

5. „Eksporter Danych" to podmiot (zewnętrzny lub wewnętrzny w ramach grupy), który dostarcza dane do Przetwarzania;

6. „Importer Danych" lub „odbiorca" to podmiot (zewnętrzny lub wewnętrzny w ramach grupy), który wykorzystuje dane do Przetwarzania;

7. „Wiążące Reguły Korporacyjne” lub „WRK” oznaczają polityki ochrony Danych Osobowych, których przestrzega Administrator lub Podmiot Przetwarzający;
8. „Członek WRK” oznacza spółkę działającą w ramach Grupy Roust jako Eksporter Danych lub Importer Danych, która uczestniczy w wewnątrzgrupowym przekazywaniu Danych Osobowych z i do UE;
9. „Organ Nadzorczy” oznacza niezależny organ publiczny utworzony przez Państwo Członkowskie jako organ odpowiedzialny za monitorowanie stosowania RODO;
10. „Kompetentny Organ Nadzorczy” oznacza wybrany Organ Nadzorczy, któremu prezentowane jest stosowanie WRK, utworzony na terytorium Państwa Członkowskiego w odniesieniu do transferu lub zbioru transferów Danych Osobowych do Administratora Danych lub Procesora w jednym lub większej liczbie krajów trzecich w ramach grupy przedsiębiorstw lub grup firm prowadzących wspólną działalność gospodarczą;
11. „Państwo Członkowskie” oznaczają kraj należący do Unii Europejskiej;

## 3. Zakres i zastosowanie

1. Zakres WRK ogranicza się do przekazywania oraz Przetwarzania Danych Osobowych, które mogą obejmować przepływy danych z i do członka WRK znajdującego się na terenie UE i prowadzącego działalność w ramach Grupy Roust. Lista członków WRK znajduje się w Załączniku A.

2. Wszelkie przypadki Przetwarzania lub przekazywania Danych Osobowych wykonywanego wewnętrznie przez członków WRK są objęte lokalnymi politykami zatwierdzonymi przez zarząd odpowiedniej spółki. Polityki te określają obowiązki zarządu i pracowników w zakresie ochrony Danych Osobowych oraz sankcje nakładane w przypadku postępowania niezgodnego z daną polityką.

3. WRK obowiązują w odniesieniu do następujących typów danych podlegających raportowaniu lub przedkładanych do celów związanych z działalnością korporacji:

- Rekrutacja pracowników (powyżej określonego poziomu zarządczego);
- Zarządzanie wynikami i rozwój zawodowy pracowników;
- Płace i zarządzanie świadczeniami pracowników (powyżej określonego poziomu zarządczego);
- Finanse korporacyjne;
- Zarządzanie bazami danych;
- Szkolenie pracowników i przedstawicieli wykonawców;
- Zarządzanie sprzedażą lub sprzedaż związana z wykorzystaniem danych osób (np. szczegółowe dzienne raporty dotyczące sprzedaży);
- Utrzymanie i rozwój relacji z klientami, w tym roszczenia i rozliczenia;
- Zarządzanie marketingiem lub zarządzanie związane z wykorzystaniem

danych osób (np. szczegółowe raporty dotyczące zdarzeń marketingowych);
- Łańcuch dostaw: zatwierdzanie faktur;
- Łańcuch dostaw: zatwierdzanie wydatków CAPEX;
- Alarmy bezpieczeństwa dotyczące obszaru ochrony środowiska i BHP;
- Informacje niezbędne do zapobiegania nadużyciom lub prowadzenia dochodzeń, albo do innych celów związanych z zarządzeniem ryzykiem;

Opis przepływów danych pomiędzy krajami przedstawiono w Załączniku B.

4. Dodatkowo Dane Osobowe są przetwarzane w układzie horyzontalnym przez wszystkich członków WRK w celu zarządzaniem tożsamością pracowników i przedstawicieli wykonawców, a także w celu realizacji usług weryfikacji informacji w systemach informatycznych Grupy Roust (np. Helpdesk).

## 4. Prawa Osób, których dotyczą dane

1. Wszyscy członkowie WRK gwarantują następujące prawa podstawowe wszystkich Osób, których dotyczą dane. Obejmuje to wszystkie spośród następujących zasad:

    a. Dane Osobowe są przekazywane i przetwarzane w konkretnych, uzasadnionych i zgodnych z prawem celach. Osoby, których dotyczą dane otrzymują wystarczające informacje, sformułowane w jednoznaczny i zrozumiały sposób (zazwyczaj w formie oświadczenia o rzetelnym Przetwarzaniu), na temat wykorzystywania ich danych oraz ich ujawniania (w tym wtórnego wykorzystywania i ujawniania ich danych), odbiorców i kategoriach odbiorców Danych Osobowych oraz tożsamości Administratora Danych w przypadku uzyskania danych przez członka WRK.

    b. Dane Osobowe są dokładne i aktualne. Każdy członek WRK zachęca Osoby, których dotyczą dane do informowania odpowiedniego Administratora Danych o wszelkich zmianach ich Danych Osobowych.

    c. Dane Osobowe są przechowywane tak długo, jak jest to konieczne. Dane Osobowe są zawsze przetrzymywane oraz/lub usuwane, w wymaganym zakresie, zgodnie z obowiązującym prawem, przepisami i standardami profesjonalnymi oraz zgodnie z lokalnymi politykami dotyczącymi retencji danych, które są wiążące dla członka WRK. Po upływie okresu retencji danych, członek WRK usuwa Dane Osobowe wyłącznie w sposób bezpieczny i zgodny z odpowiednią lokalną polityką bezpieczeństwa.

    d. Dane Osobowe są gromadzone i przetwarzane w minimalnym zakresie niezbędnym do osiągnięcia celu Przetwarzania.

e. Dane wrażliwe[1] są wykorzystywane wyłącznie wtedy, gdy jest to absolutnie konieczne. W takim przypadku dostęp do wrażliwych danych osobowych jest ograniczony do odpowiednich osób (poprzez maskowanie lub anonimizację danych, stosownie do sytuacji).

f. Dane Osobowe nie są przesyłane do podmiotów zewnętrznych bez zapewnienia odpowiedniej ochrony tych danych.

2. Osoba, której dotyczą dane ma prawo do dostępu, poprawiania, usuwania, ograniczania, a także sprzeciwu wobec Przetwarzania. Wyżej wymienione prawa nie są zależne od decyzji opartych wyłącznie na przetwarzaniu automatycznym, w tym profilowania. Procedura udzielania dostępu została opisana w Załączniku C.

3. Osoba, której dotyczą dane ma prawo do złożenia skargi w ramach wewnętrznego mechanizmu obsługi skarg każdego członka WRK. Ponadto, Osoba, której dotyczą dane ma możliwość złożenia skargi do w kompetentnego Organu Nadzorczego, stosownie do miejsca zamieszkania Osoby, której dotyczą dane, jej miejsca pracy lub miejsca rzekomego naruszenia jej praw, albo w sądzie w dowolnym Państwie Członkowskim UE wybranym przez Osobę, której dane dotyczą. Procedura rozpatrywania skarg została opisana szczegółowo w Załączniku D.

4. W przypadku potencjalnego lub faktycznego naruszenia Danych Osobowych, dany członek WRK ma obowiązek postępowania zgodnie z procedurą określoną w niniejszych WRK, w Załączniku E, a także obowiązek współpracy w najszerszym możliwym zakresie z Organem Nadzorczym, którego sprawa dotyczy.

5. Osoba, której dotyczą dane ma prawo do działań prawnych oraz prawo do uzyskania zadośćuczynienia, a także, tam gdzie jest to właściwe, odszkodowania w przypadku naruszenia postanowień WRK określonych w punkcie 4, par. 1, p. a-f powyżej.

## 5. Transparentność i prawo do informacji

1. Przed rozpoczęciem przetwarzania ich danych, Osoby, których dotyczą dane uzyskują następujące informacje:
   a. Tożsamość Administratora/Administratorów oraz jego/ich przedstawicieli, jeśli istnieją;
   b. Cele Przetwarzania danych;
   c. Ewentualne dodatkowe informacje, takie jak:

[1] Dane wrażliwe to dane dotyczące rasy lub pochodzenia etnicznego, przekonań politycznych, religijnych i innych, członkowstwa w związkach zawodowych, zdrowia, życia seksualnego, wyroków skazujących w postępowaniach karnych, dokumenty ubezpieczenia społecznego, rządowe numery identyfikacyjne oraz numery rachunków finansowych.

i) odbiorcy lub kategorie odbiorców danych;

ii) istnienie prawa dostępu do danych oraz prawa do korygowania danych dotyczących wyłącznie danej Osoby, której dane dotyczą;

iii) warunki uznania żądania przez Osobę, której dane dotyczą, zaprzestania lub zablokowania Przetwarzania, w tym usunięcia danych, jeśli będzie to konieczne;

iv) zgodne z prawem procedury postępowania (zarówno dla Osób, których dane dotyczą, od których dane są pozyskiwane bezpośrednio, jak i dla beneficjentów będących osobami trzecimi, np. są klientami Eksportera Danych).

2. Każda Osoba, której dotyczą dane, ma prawo do łatwego uzyskania dostępu do swoich danych.

3. Każdy członek WRK gromadzi, przekazuje i przetwarza Dane Osobowe wyłącznie w wyraźnie określonych i zgodnych z prawem celach, zgodnie z postanowieniami WRK. W przypadku uzyskania Danych Osobowych od osób trzecich (w tym klientów członków WRK) a także z publicznie dostępnych źródeł, zawsze wykorzystywane są źródła, które są wiarygodne i cieszą się dobrą reputacją.

4. Członek WRK przekazuje Dane Osobowe wyłącznie wtedy, gdy:

   a. spełnione zostały wszystkie obowiązujące wymogi prawne;

   b. przekazanie dokonywane jest na podstawie jednoznacznie określonej potrzeby biznesowej;

   c. Importer Danych wdrożył odpowiednie środki bezpieczeństwa;

5. Członek WRK nie ujawnia Danych Osobowych z wyjątkiem sytuacji określonych w WRK, jego politykach, lub zgodnie z wymogami lub w sytuacjach dopuszczalnych na podstawie umowy lub obowiązujących przepisów.

## 6. Organizacja ochrony danych

1. Do pełnienia roli Głównego Inspektora Ochrony Danych („GIOD" lub „Główny IOD") zostaje wyznaczony Dyrektor ds. Bezpieczeństwa i Zgodności w spółce CEDC International Sp. z o.o. (będącej członkiem WRK w Polsce).

2. Obowiązki GIOD obejmują:

   a. ogólny nadzór nad realizacją postanowień WRK;

   b. doradzanie i udzielanie wsparcia Zarządowi Roust Corporation w odniesieniu do wszystkich aspektów WRK;

c. monitorowanie i raportowanie w sprawie zgodności z przepisami na poziomie korporacji;

d. wsparcie lokalnych IOD i współpraca w postępowaniu z incydentami dotyczącymi zakresu WRK;

e. obsługę dochodzeń prowadzonych przez Organa Nadzorcze.

3. GIOD podlega bezpośrednio Zarządowi Roust Corporation.

4. Członek WRK może wyznaczyć lokalnego Inspektora Ochrony Danych („IOD"). Jeśli do pełnienia tej roli nie zostanie wyznaczona inna osoba, zadania Inspektora Ochrony Danych wykonuje wyznaczony menedżer. Listę osób wyznaczonych do pełnienia roli IOD prowadzi Główny IOD.

5. Obowiązki IOD obejmują:

a. monitorowanie ochrony, przetwarzania i przekazywania danych w zakresie WRK na poziomie lokalnym;

b. prowadzenie audytów zgodnie z programem audytów WRK;

c. obsługa lokalnych skarg od Osób, których dotyczą dane w zakresie WRK;

d. obsługa incydentów związanych z zakresem WRK na poziomie lokalnym i współpraca z innymi IOD oraz Głównym IOD, tam gdzie jest to istotne;

e. zgłaszanie GIOD poważnych problemów dotyczących prywatności;

f. organizacja i monitorowanie szkoleń na poziomie lokalnym;

g. pomoc odpowiedniemu Organowi Nadzorczemu w prowadzeniu audytów lub dochodzeń, a także wdrażanie porad lub zaleceń Organu Nadzorczego.

## 7. Środki bezpieczeństwa i ich skuteczność

1. Członek WRK stosuje odpowiednie techniczne, organizacyjne, administracyjne i fizyczne środki bezpieczeństwa w celu ochrony Danych Osobowych przed nieupoważnionym lub nieuprawnionym Przetwarzaniem oraz przed przypadkową utratą lub zniszczeniem.

2. W każdym przypadku transgranicznego przekazywania Danych Osobowych pomiędzy członkami WRK stosowane są zabezpieczenia w postaci odpowiednich technik kryptograficznych zapewniających poufność danych.

3. Uprawnienia do uczestniczenia w wymianie danych pomiędzy członkami WRK ma wyłącznie odpowiednio upoważniony personel.

4. Odpowiedzialność za monitorowanie, regularne przeglądy, a także doskonalenie systemu, polityk i procedur bezpieczeństwa z uwzględnieniem pojawiających się zagrożeń, jak również nowych zabezpieczeń technologicznych i środków ostrożności ponoszą odpowiednie działy IT.

5. W przypadku powierzenia Przetwarzania Danych Osobowych przez członka WRK osobie trzeciej, dany członek WRK wybiera do tego celu rzetelne osoby trzecie, które wdrożyły odpowiednie środki bezpieczeństwa. W szczególności, dana osoba trzecia ma obowiązek niezwłocznego zgłaszania wszelkich naruszeń Danych Osobowych członkowi WRK w UE oraz odpowiedniemu Inspektorowi Ochrony Danych, a także Osobom, których dotyczą dane, jeśli naruszenie Danych Osobowych może spowodować powstanie dużego ryzyka dla ich praw i wolności.

6. Wszelkie naruszenia Danych Osobowych związane z WRK (tzn. fakty dotyczące naruszenia Danych Osobowych, jego skutki oraz podjęte działania naprawcze) są dokumentowane, a dokumentacja jest udostępniana Organowi Nadzorczemu.

7. Zapewniane jest odpowiednie szkolenie w zakresie WRK dla personelu mającego stały lub regularny dostęp do Danych Osobowych, który uczestniczy w gromadzeniu danych lub w opracowaniu narzędzi służących do przetwarzania Danych Osobowych.

8. Wszelkie aspekty WRK, w tym metody zapewnienia podjęcia działań naprawczych, podlegają regularnie prowadzonym audytom.

9. Ogólny program audytów dotyczących WRK jest opracowywany przez Głównego Inspektora Ochrony Danych i realizowany po zatwierdzeniu przez Zarząd Roust Corporation.

10. Wyniki wszystkich audytów są przekazywane Głównemu Inspektorowi Ochrony Danych.

11. Główny Inspektor Ochrony Danych albo odpowiedni lokalny Inspektor Ochrony Danych zapewnia , aby odpowiedni Organ Nadzorczy miał, na swoje żądanie, dostęp do wyników audytu i pomaga Organowi Nadzorczemu w realizacji audytu ochrony danych u dowolnego członka WRK, jeśli zajdzie taka konieczność.

## 8. Rozliczalność i zgodność z przepisami

1. Każdy członek WRK pełniący obowiązki Administratora Danych ma obowiązek zapewnienia i wykazania zgodności z WRK.

2. W celu wykazania zgodności, członkowie WRK z UE prowadzą rejestr wszystkich kategorii prowadzonych czynności przetwarzania, zgodnie z wymaganiami określonymi w RODO. Dokumentacja ta jest udostępniana odpowiedniemu Organowi Nadzorczemu na jego żądanie.

3. Wdrożone są odpowiednie środki techniczne i organizacyjne w celu zapewnienia przestrzegania głównych zasad ochrony danych, tzn. privacy by design oraz privacy by default.

4. Ocena wpływu na ochronę danych jest prowadzona w przypadku spełnienia konkretnych kryteriów, o których mowa w RODO.

## 9. Obowiązujące prawo i odpowiedzialność

1. WRK są zgodne z odpowiednimi przepisami UE, w szczególności z Rozporządzeniem o Ochronie Danych Osobowych („RODO") oraz lokalnym prawem krajów, w których działalność prowadzą spółki Grupy Roust.

- 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 (Rozporządzenie o Ochronie Danych Osobowych, RODO)
- Ustawa o prywatności (R.S.C., 1985, c. P-21) (Kanada)
- Ustawa o ochronie danych osobowych i dokumentach elektronicznych (PIPEDA) (Kanada)
- PROJEKT USTAWY ZMIENIAJĄCEJ WĘGIERSKIE PRZEPISY W SPRAWIE OCHRONY DANYCH (Węgry)
- Projekt Ustawy o ochronie danych osobowych (Polska)
- Ustawa federalna z dnia 27 lutego 2006 r. N 152-FZ O DANYCH OSOBOWYCH (Rosja)
- Ustawa Federalna nr 242-FZ z dnia 21 lipca 2014 r. w sprawie zmiany niektórych aktów prawnych Federacji Rosyjskiej w zakresie, w jakim dotyczy to aktualizacji procedury przetwarzania danych osobowych w sieciach teleinformatycznych (wraz ze zmianami i uzupełnieniami) (Rosja)
- Ustawa o ochronie danych osobowych (Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481) (Ukraina)
- Dekret w sprawie uzgodnienia treści dokumentów w obszarze ochrony danych osobowych, НАКАЗ 08.01.2014 № 1/02-14 (Ukraina)

2. Jeśli lokalne przepisy wymagają wyższego poziomu ochrony Danych Osobowych, przepisy takie mają pierwszeństwo przed WRK.

3. Każdy członek WRK z UE eksportujący dane poza UE na podstawie WRK odpowiada za wszelkie naruszenia WRK przez członka WRK mającego siedzibę poza UE, który otrzymuje dane od tego członka WRK.

4. Członek WRK, który przyjął odpowiedzialność, musi także udowodnić, że członek WRK spoza UE nie odpowiada za jakiekolwiek naruszenia zasad

będące przyczyną roszczenia odszkodowania przez Osobę, której dotyczą dane. W przypadku udowodnienia takiego stanu rzeczy, dany członek WRK nie ponosi żadnej odpowiedzialności.

## 10. Wyjątki od obowiązku przestrzegania WRK

1. Jeśli członek WRK ma podstawy do uznania, że obowiązujące go przepisy uniemożliwiają firmie realizację jej obowiązków wynikających z WRK lub mają istotny wpływ na gwarancje zapewnione przez te zasady, wówczas niezwłocznie informuje on Głównego Inspektora Ochrony Danych oraz odpowiedniego Inspektora Ochrony Danych, chyba że zabroni tego odpowiedni organ ścigania, np. zgodnie z obowiązującym prawem karnym w celu ochrony poufności śledztwa prowadzonego przez ten organ ścigania.

2. Co więcej, jeśli jakikolwiek wymóg prawny, któremu podlega członek WRK w dowolnym kraju trzecim, może mieć istotny niekorzystny wpływ na gwarancje, jakie zapewnia WRK, wówczas problem ten należy zgłosić odpowiedniemu Organowi Nadzorczemu. Obejmuje to każde wiążące prawnie żądanie ujawnienia Danych Osobowych ze strony organu ścigania lub państwowego organu bezpieczeństwa. W takim przypadku Organ Nadzorczy zostaje jednoznacznie poinformowany o takim żądaniu, w tym uzyska informacje o żądanych danych, organie składającym żądanie oraz podstawie prawnej ujawnienia (chyba że jest to zabronione z innych powodów, np. zgodnie z prawem karnym, w celu zachowania poufności dochodzenia prowadzonego przez organa ścigania).

3. Jeśli w określonych przypadkach takie zawieszenie lub powiadomienie są zabronione przez prawo, wówczas dany członek WRK podejmuje wszelkie działania w celu uzyskania prawa do rezygnacji z zakazu w celu przekazania takich informacji oraz może, tak szybko jak będzie to możliwe, wykazać, że podjął takie działania.

4. Jeśli we wszystkich powyższych przypadkach dany członek WRK nie jest w stanie powiadomić danego Organu Nadzorczego, wówczas ma on obowiązek corocznego przekazywania ogólnych informacji na żądanie Organu Nadzorczego (np. liczba wniosków o ujawnienie, rodzaj żądanych danych, osoba wnioskująca, jeśli jest to możliwe).

5. W żadnym przypadku przekazanie Danych Osobowych przez członka WRK dowolnemu organowi publicznemu nie może być masowe, nieproporcjonalne i bezkrytyczne, ani odbywać się w sposób wychodzący poza zakres niezbędny w demokratycznym społeczeństwie.

## 11. Aktualizacja WRK

1. WRK zostaną zmodyfikowane w przypadku spełnienia co najmniej jednego z następujących warunków:

- wymagane są istotne zmiany w samych WRK;

- zmiany środowiska prawnego w zakresie praw i obowiązków Organów Nadzorczych;

- zmiany w spółce lub strukturze korporacyjnej skutkujące nowymi upoważnieniami/dopuszczeniami ze strony Organu Nadzorczego.

2. Jeśli modyfikacja mogłaby wpłynąć na poziom ochrony zapewniany przez WRK lub znacznie wpłynąć na WRK (tzn. zmiany jego wiążącego charakteru), konieczne jest niezwłoczne poinformowanie odpowiednich Organów Nadzorczych za pośrednictwem kompetentnego Organu Nadzorczego.

3. Po zatwierdzeniu przez Zarząd Roust Corporation, Główny Inspektor Ochrony Danych ma obowiązek niezwłocznego informowania o zmianach wszystkich członków WRK oraz odpowiednie Organa Nadzorcze za pośrednictwem kompetentnego Organu Nadzorczego.

4. Następujące zmiany WRK nie powodują konieczności ponownego wniosku o dopuszczenie przez kompetentny Organ Nadzorczy:

- Główny Inspektor Ochrony Danych prowadzi w pełni zaktualizowaną listę członków WRK i śledzi oraz zapisuje wszelkie zmiany zasad, a także przekazuje Osobom, których dotyczą dane lub Organom Nadzorczym, na ich żądanie, niezbędne informacje;

- Dane Osobowe nie są przekazywane nowemu członkowi WRK do czasu, gdy nowy członek WRK zostanie skutecznie związany przez postanowienia WRK i będzie w stanie wykazać spełnienie tych postanowień;

- wszelkie zmiany w WRK lub w liście członków WRK są zgłaszane raz w roku do odpowiedniego Organu Nadzorczego, z pośrednictwem kompetentnego Organu Nadzorczego, z krótkim wyjaśnieniem przyczyn uzasadniających aktualizację.

## Załącznik A - Lista członków WRK

| | |
|---|---|
| Roust Corporation | CEDC International sp. z o.o |
| 232 Madison Avenue, Suite 1600, NY 10016 New York, USA | ul. Kowanowska 48, 64-600 Oborniki, Polska |
| PWW sp. z o. o. | B2B Wine & Spirits sp. z o.o. |
| ul. Bobrowiecka 8, 00-728 Warszawa, Polska | Lubińska 10, 05-532 Lubna, Polska |
| ROUST Hungary Kft. | ROUST UKRAINE LLC |
| Alkotás u. 50 1123 Budapeszt, Węgry | Konstantinovskaya str., 2A, 04071, Kijów, Ukraina |
| JSC «Roust Russia» | „Parliament Production", LLC |
| Eniseiskaya str., b. 1, con. 1, 129344, Moskwa, Federacja Rosyjska | Balashiha, microregion Saltikovka, Popovka str., ownership 5, 143916, Region Moskiewski, Federacja Rosyjska |
| „Russian Standard Vodka" LLC | Bravo Premium LLC |
| Pulkovskoe shosse 46, build 2, 196140, Sankt Petersburg, Federacja Rosyjska | ul. Kuznetsovskaya, b. 52, con.3, letter A, 196105, Sankt Petersburg, Federacja Rosyjska |
| CJSC „ROUST INC." | Roust Distribution Limited |
| Shoushari village, Pulkovskoe road, b.52, letter A, 196140, Sankt Petersburg, Federacja Rosyjska | Diagorou 4, Kermia, Building, 6th floor, Office 601, Nicosia, P.C. 1097, Cypr |
| Roust Distribution (Brytyjski oddział ROUST DISTRIBUTION LIMITED) | Russian Standard Vodka (USA), Inc. |
| Thomas House, 84 Eccleston Square, London, United Kingdom, SW1V 1PX | c/o Corporation Service Company, 2711 Centerville Road, Suite 400, in the City of Wilmington, County of New Castle, Delaware, USA |
| JOINT STOCK COMPANY "DISTILLERY TOPAZ" | „Trading House „Russian Alcohol – Moscow" LLC |
| 46, Oktyabrskaya str., Pushkin, Region Moskiewski, 141200, Federacja Rosyjska | 1/1, Eniseyskaya str., Moskwa, 129344, Federacja Rosyjska |
| Russian Standard Vodka Canada Ltd. | F.lli Gancia & c. spa |
| Suite 4000, Bay street, 199, Toronto, Ontario, Kanada, M5L 1A9 | Corso liberta 66, 14053 Canelli, Asti, Włochy |

## Załącznik B - Opis przepływów danych

Prezentacja przepływów danych w zakresie istotnej wymiany transgranicznej pomiędzy członkami WRK (z podziałem na kraje)

| Typy danych przekazywanych do lub zawartych w raportach składanych w Centrali Korporacji lub podlegające wymianie wewnątrz grupy*, które mogą wiązać się z danymi osobowymi | Spółki w kraju | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Rosja | Polska | Ukraina | Wielka Brytania/Cypr | USA/Kanada | Węgry | Włochy | Uwagi dotyczące konkretnego kraju |
| Rekrutacja pracowników - powyżej określonego poziomu zarządczego | nie | tak | tak | tak | tak | tak | nie | |
| Zarządzanie wynikami i rozwój zawodowy pracowników; | nie | nie | tak | nie | tak | tak | tak | |
| Płace i zarządzanie świadczeniami pracowników - powyżej określonego poziomu zarządczego | tak | tak | tak | tak | tak | tak | tak | |
| Finanse korporacyjne; | tak | tak | tak | nie | tak | tak | tak | |
| Zarządzanie bazami danych; | nie | nie | | tak | nie ma odniesienia | tak | tak | Węgry: właścicielem podmiotu prawnego na Węgrzech jest CEDC i dlatego takie dane i inne podobne dane mogą być przekazywane do CEDC |
| Szkolenie pracowników i przedstawicieli wykonawców; | nie | nie | tak | nie | nie | nie | nie | |
| Zarządzanie sprzedażą lub sprzedaż związana z wykorzystaniem danych osób (np. szczegółowe dzienne raporty dotyczące sprzedaży); | nie | tak | tak | nie | nie | nie | nie | Węgry: dane takie są zawarte w raportach, ale nie pokazują dane na poziomie poszczególnych sprzedawców |
| Utrzymanie i rozwój relacji z klientami, w tym roszczenia i rozliczenia; | nie | nie | tak | nie | nie ma odniesienia | nie | nie | |
| Zarządzanie marketingiem lub zarządzanie związane z wykorzystaniem danych osób (np. szczegółowe raporty dotyczące zdarzeń marketingowych); | nie ma odniesienia | nie | *nie* | nie | tak | nie | nie | USA - w przypadku modeli promocyjnych, na fakturach podawane są nazwiska osób |
| Łańcuch dostaw: zatwierdzanie faktur; | nie | tak | tak | nie | nie | nie | nie ma odniesienia | |
| Łańcuch dostaw: zatwierdzanie wydatków CAPEX; | nie | tak | tak | nie | nie | tak | nie | |
| Alarmy bezpieczeństwa dotyczące obszaru ochrony środowiska i BHP; | nie | tak | tak | nie ma odniesienia | nie ma odniesienia | nie | nie ma odniesienia | |
| Niezbędne do zapobiegania nadużyciom lub prowadzenia dochodzeń, albo do innych celów związanych z zarządzeniem ryzykiem; | nie | nie | tak | nie | tak | nie | nie | US - w ramach dochodzenia dotyczącego oszustw związanych z użyciem kart kredytowych, informacje przekazano audytorowi |
| W celu identyfikacji (zarządzanie tożsamości pracowników oraz przedstawicieli wykonawców), a także w celu weryfikacji informacji (np. Helpdesk); | tak | tak | tak | nie | tak | tak | tak | |

* Pomiędzy wszystkimi lub niektórymi spółkami w Roust Corporation

| Odpowiedź | Znaczenie |
|---|---|
| tak | raporty mogą zawierać dane osobowe (np. dane pracowników lub klientów) |
| nie | raporty są agregowane i nie zawierają danych osobowych |
| Nie ma odniesienia | ten typ danych nie jest przetwarzany w danym rozdziale |

# Załącznik C - Procedura żądania dostępu od Osoby, której dotyczą dane

## Wprowadzenie

Europejskie przepisy o Ochronie Danych dają osobom, których Dane Osobowe są gromadzone oraz/lub przesyłane na terytorium UE prawo do bycia informowanymi o tym, czy ich Dane Osobowe są przetwarzane przez organizację. Zgodnie z art. 15 RODO, Osoba, której dotyczą dane ma prawo dostępu do następujących informacji:

(a) cele przetwarzania;
(b) kategorie odnośnych danych osobowych;
(c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
(d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
(e) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
(f) informacje o prawie wniesienia skargi do organu nadzorczego;
(g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
(h) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Dodatkowo, jeśli Dane Osobowe są przekazywane do kraju trzeciego lub do organizacji międzynarodowej, Osoba, której dane dotyczą ma prawo do uzyskania informacji o odpowiednich zabezpieczeniach.

Wszystkie Osoby, których dane dotyczą, których Dane Osobowe są gromadzone i wykorzystywane na terytorium UE **oraz dodatkowo** przekazywane pomiędzy członkami WRK, mają prawo do dostępu zgodnie z warunkami niniejszej procedury. Tam, gdzie obowiązujące przepisy o ochronie danych poza UE różnią się w dowolnym aspektu tej procedury, pierwszeństwo mają te lokalne przepisy o ochronie danych.

## Postanowienia ogólne

1. Żądanie należy złożyć na piśmie, co może obejmować także pocztę elektroniczną.
2. Przedmiotem procedury są żądania dostępu składane przez Osoby, których dane dotyczą, dotyczące zakresu WRK (ważne żądanie).
3. Żaden członek WRK nie ma obowiązku spełnienia żądania, zanim Osoba, której dotyczą dane, która złożyła żądanie, nie przedstawi racjonalnego potwierdzenia swojej tożsamości.
4. Członek WRK udziela odpowiedzi na ważne żądanie w ciągu 30 dni kalendarzowych (lub w krótszym terminie określonym w lokalnych przepisach) od otrzymania żądania.
5. W normalnych okolicznościach nie jest naliczana żadna opłata, jednak decyduje o tym członek WRK, u którego złożono żądanie, zgodnie z obowiązującymi przepisami lokalnymi.

## Otrzymywanie i akceptacja żądania

6. W przypadku otrzymania przez jakiegokolwiek pracownika, wspólnika lub podwykonawcę członka WRK jakiegokolwiek żądania od osoby fizycznej dotyczącego udzielenia dostępu do jej Danych Osobowych, taka wiadomość jest niezwłocznie przekazywana do odpowiedniego lokalnego IOD wraz z datą otrzymania oraz wszelkimi innymi informacjami które mogą pomóc IOD w odniesieniu się do żądania.
7. Lokalny IOD dokonuje wstępnej oceny żądania i decyduje o tym, czy jest to ważne żądanie.
8. Lokalny IOD kontaktuje się z osobą, która złożyła żądanie na piśmie w celu wykonania co najmniej jednej z następujących czynności:
    a. Potwierdzenia odbioru żądania w celu dalszego Przetwarzania;
    b. Prośby o dodatkowe informacje, w tym potwierdzenia tożsamości;
    c. Odmowy spełnienia żądania jeśli w jego ocenie jest ono nieważne.
9. Zgodnie z p. 8.c, podstawą odmowy spełnienia żądania może być co najmniej jedna z następujących sytuacji:
    a. Jeśli żądanie złożono u członka WRK i dotyczy ono użycia lub gromadzenia Danych Osobowych przez tego członka, a odmowa udzielenia informacji jest zgodna z przepisami o ochronie danych obowiązującymi w danej jurysdykcji;
    b. W opinii członka WRK:
        i. spełnienie żądania byłoby niekorzystne dla podstawowych interesów biznesowych członka WRK (co obejmuje planowanie zarządcze, finanse korporacyjne lub negocjacje z

Osobą, której dotyczą dane, która złożyła wniosek);

ii. jest to konieczne ze względu na bezpieczeństwo publiczne, obronę, bezpieczeństwo narodowe oraz działania państwa w obszarze prawa karnego;

iii. jest to konieczne dla ochrony samej Osoby, której dotyczą dane albo praw i wolności innych osób;

c. Jeśli Dane Osobowe są w posiadaniu członka WRK w formie niezautomatyzowanej i nie są, ani nie staną się one częścią systemu rejestracji danych;

d. Jeśli dostarczenie Danych Osobowych wymaga od członka WRK nieproporcjonalnego wysiłku.

10. Lokalny IOD może w przypadku złożonych spraw zwrócić się do Głównego IOD o radę, w szczególności jeśli żądanie obejmuje informacje dotyczące osób trzecich lub jeśli przekazanie Danych Osobowych może mieć negatywny wpływ na poufność działalności biznesowej lub postępowania prawne.

## Wyszukiwanie i odpowiedź

11. Lokalny IOD organizuje przeszukiwanie wszystkich istotnych elektronicznych i papierowych systemów rejestracji danych.

12. Informacje będące przedmiotem żądania są przekształcane przez lokalnego IDO do formatu łatwego do zrozumienia (np. kody wewnętrzne lub numery identyfikacyjne odpowiadające Danym Osobowym są usuwane przed przesłaniem do Osoby, której dane dotyczą). Następnie, lokalny IOD przesyła do Osoby, której dane dotyczą wszystkie informacje, które muszą być przekazane w odpowiedzi na żądanie.

13. Jeśli dostarczenie informacji w formie utrwalonej nie jest możliwe lub wiązałoby się z nieproporcjonalnym nakładem pracy, nie ma obowiązku dostarczenia utrwalonego egzemplarza informacji. W takich okolicznościach osoba może uzyskać możliwość dostępu do informacji w drodze inspekcji lub zdalnego dostępu do bazy danych, albo otrzymać informacje w innej formie.

## Żądania usunięcia, zmiany lub zaprzestania przetwarzania informacji

14. W przypadku otrzymania od osoby fizycznej żądania usunięcia Danych Osobowych tej osoby, takie żądanie jest rozpatrywane przez lokalnego IOD. Jeśli Przetwarzanie jest prowadzone na innej ważnej i zgodnej z prawem podstawie, takie żądanie jest odrzucane.

15. W przypadku otrzymania od osoby fizycznej żądania zmiany Danych Osobowych tej osoby, informacje takie należy poprawić lub zaktualizować, jeśli istnieje zgodna z prawem podstawa do takiego działania.

16. W przypadku żądania zaprzestania przetwarzania Danych Osobowych osoby fizycznej z powodu zagrożenia dla praw i wolności tej osoby z

powodu takiego Przetwarzania przez członka WRK, żądanie takie jest przekazywane przez lokalnego IOD do Głównego IOD do dalszej oceny. Jeśli Przetwarzanie prowadzone przez członka WRK jest wymagane z uwagi na jakąkolwiek podstawę prawną, żądanie takie jest odrzucane.

# Załącznik D - Procedura rozpatrywania skarg

## Wprowadzenie

Jeśli Osoba, której dane dotyczą uzna, że jej Dane Osobowe są przetwarzane z naruszeniem WRK, osoba taka może zgłosić swoje obawy do członka WRK w formie pisemnej, pocztą elektroniczną lub w inny sposób określony w WRK z wykorzystaniem danych kontaktowych podanych w Załączniku A do WRK.

Celem tej procedury jest wyjaśnienie sposobu obsługi skarg składanych przez osoby, których Dane Osobowe są przetwarzane przez członka WRK oraz w zakresie WRK.

## Postępowanie ze skargami

1. W przypadku otrzymania przez jakiegokolwiek pracownika, wspólnika lub podwykonawcę członka WRK jakiejkolwiek skargi dotyczącej WRK, taka wiadomość jest niezwłocznie przekazywana do odpowiedniego lokalnego IOD wraz z datą otrzymania oraz wszelkimi innymi informacjami, które mogą pomóc IOD w rozpatrzeniu skargi.
2. Lokalny IOD przesyła do danej osoby potwierdzenie otrzymanie skargi w ciągu 5 dni roboczych.
3. Lokalny IOD rozpatruje skargę, korzystając ze wsparcia odpowiednich jednostek biznesowych i innych jednostek organizacyjnych, a także wsparcia Głównego IOD, jeśli zajdzie taka konieczność.
4. W normalnych okolicznościach lokalny IOD przygotowuje odpowiedź i przekazuje ją danej osobie w ciągu 30 dni. W przypadku braku możliwości udzielenia odpowiedzi w tym terminie z uwagi na złożoność skargi, lokalny IOD informuje o tym daną osobę i przekazuje racjonalnie oszacowany termin udzielenia odpowiedzi. W żadnym wypadku termin ten nie może przekroczyć sześciu miesięcy od daty złożenia skargi.

## Rozstrzyganie sporów

5. W przypadku zakwestionowania przez osobę, która złożyła skargę udzielonej odpowiedzi lub jakiegokolwiek aspektu ustaleń lokalnego IOD, kwestia ta jest przekazywana Głównemu IOD, który dokonuje przeglądu sprawy i podejmuje decyzję o potwierdzeniu udzielonej odpowiedzi lub o udzieleniu nowej odpowiedzi.
6. Główny IOD podejmuje wszelkie uzasadnione działania w celu rozstrzygnięcia sporu.
7. Działania Głównego IOD muszą zostać zakończone w terminie 60 dni od daty ponownego złożenia skargi.

## Postanowienia końcowe

Niezależnie od opisanej powyżej procedury, osoba, której Dane Osobowe są gromadzone oraz/lub wykorzystywane, ma prawo do złożenia skargi w wybranym Organie Nadzorczym, w szczególności w Państwie Członkowskim, w którym znajduje się jego miejsce zamieszkania lub miejsce pracy, a także prawo do skutecznych środków prawnych zgodnie z postanowieniami RODO, co obejmuje

przypadki, w których nie jest ona usatysfakcjonowana rozstrzygnięciem w sprawie skargi dotyczącego WRK.

Osoby posiadające takie prawo są odpowiednio powiadamiane o tym fakcie w ramach procedury rozpatrywania skarg.

# Załącznik E - Procedura postępowania z incydentami

## Wprowadzenie

Naruszenie danych osobowych (w dalszej części niniejszego dokumentu określane jako incydent) może mieć miejsce z wielu powodów, np.:

- utraty lub kradzieży danych lub wyposażenia, na którym dane są przechowywane lub przez które może być uzyskany dostęp do nich;
- utraty lub kradzieży plików papierowych;
- nieautoryzowanego dostępu do danych (np. w wyniku ataku hakerskiego);
- nieodpowiedniej kontroli dostępu umożliwiającej nieupoważniony/niepotrzebny dostęp do danych;
- awarii wyposażenia;
- błędu administratora lub użytkownika;
- nieprzewidzianych okoliczności, takich jak pożar lub powódź;

Rozporządzenie o Ochronie Danych Osobowych stwierdza, że natychmiast po tym, jak Administrator Danych (w zakresie WRK - członek WRK, którego sprawa dotyczy) dowie się o wystąpieniu naruszenia Danych Osobowych, taki incydent powinien zostać zgłoszony do Organu Nadzorczego niezwłocznie lecz, jeśli jest to możliwe, nie później niż 72 godziny po potwierdzeniu informacji o incydencie, chyba że dany członek WRK z UE jest w stanie wykazać, zgodnie z zasadą rozliczalności, że jest mało prawdopodobne, iż naruszenie danych osobowych spowoduje ryzyko dla praw i wolności osób fizycznych.

## Zgłaszanie incydentu

1. W przypadku stwierdzenia wystąpienia lub podejrzenia naruszenia Danych Osobowych, zostaje ono niezwłocznie zgłoszone do lokalnego IOD.
2. W celu poprawy ogólnego zrozumienia ryzyka dla Danych Osobowych i reagowania na nie przed wystąpieniem naruszeń, każdy pracownik, wspólnik lub podwykonawca jest zachęcany do zgłaszania „sytuacji grożących naruszeniem" (tzn. incydentów, które spowodowałyby naruszenie Danych Osobowych gdyby nie podjęto interwencji lub gdyby nie zwykłe „szczęście").

## Dochodzenie w sprawie incydentu

3. Lokalny IOD przeprowadza pierwszą ocenę incydentu.
4. Jeśli incydent wpływa na transgraniczną wymianę Danych Osobowych, lokalny IOD niezwłocznie informuje o nim IOD działających u odpowiednich członków WRK oraz Głównego IOD. Pracę zespołu IOD koordynuje lokalny IOD działający u danego członka WRK w UE lub Główny IOD, tam gdzie jest to wymagane.
5. Zespół IOD działających u odpowiednich członków WRK prowadzi dalszą analizę sprawy i podejmuje decyzję o tym, czy wymagane są jakiekolwiek natychmiastowe działania naprawcze/ ograniczające/ eskalacyjne.

6. Zależnie od typu i powagi incydentu i stosownie do decyzji zespołu IOD działających u odpowiednich członków WRK, lokalny IOD lub Główny IOD, zależnie od tego, kto został wyznaczony do pełnienia roli koordynatora zespołu:
    - Aktualizuje rejestr naruszeń Danych Osobowych i zamyka zapis w rejestrze, jeśli incydent nie wymaga dalszej oceny albo
    - Rozpoczyna dochodzenie i wyznacza odpowiedni zespół dochodzeniowy składający się z odpowiednich ekspertów wewnętrznych lub zewnętrznych (np. z działów IT danych członków WRK);
    - Monitoruje działania zespołu dochodzeniowego i prowadzi bieżącą ocenę incydentu.
7. W wyniku dochodzenia następuje:
    - Określenie charakteru i zakresu incydentu, typu i ilości danych, których incydent dotyczy, a także tożsamości Osób, których dane dotyczą;
    - Przeprowadzenie oceny ryzyka dla praw i wolności Osób, których dane dotyczą;
    - Określenie działań, które muszą podjąć odpowiedni członkowie WRK w celu ograniczenia naruszenia i odzyskania informacji;
    - Przedstawienie zaleceń dotyczących działań niezbędnych do zapobieżenia ponownemu wystąpieniu incydentu w przyszłości.
8. Jeśli bieżące oceny wykażą, że incydentu nie można ograniczyć w odpowiednim czasie, informowany jest o tym Główny IOD oraz kierownictwo danych członków WRK z UE.
9. Zależnie od wyników dochodzenia, lokalny IOD lub Główny IOD, tam gdzie jest to wymagane, sporządza pełen raport ex-post z naruszenia i aktualizuje rejestr naruszeń Danych Osobowych.

## Zgłaszanie naruszenia odpowiedniemu Organowi Nadzorczemu lub Osobom, których dotyczą dane

10. Jeśli w wyniku oceny ryzyka dla praw i wolności Osób, których dotyczą dane stwierdzone zostanie to, że ryzyko to jest wysokie, lokalny IOD działający u danego członka WRK z UE lub Główny IOD, tam gdzie jest to konieczne, koordynuje zgłoszenie incydentu odpowiedniemu Organowi Nadzorczemu. Informowane jest także kierownictwo danych członków WRK lub Zarząd Korporacji, tam gdzie jest to właściwe.
11. Co więcej, w takim przypadku o incydencie niezwłocznie są informowane również Osoby, których dotyczą dane. Taką kampanię informacyjną koordynuje lokalny IOD działający u danego członka WRK z UE lub Główny IOD, tam gdzie jest to wskazane, który korzysta ze wsparcia odpowiednich działów prawnych oraz/lub PR.

## Działania po incydencie

Po zamknięciu postępowania w sprawie incydentu, Główny IOD sprawdza rejestr naruszeń Danych Osobowych lub raport ex-post z naruszenia w celu określenia tego, czy konieczna jest aktualizacja WRK. Główny IOD koordynuje ewentualne szkolenia i komunikację związaną z wyciągniętymi wnioskami.