POLITYKA BEZPIECZEŃSTWA

PRZETWARZANIA DANYCH OSOBOWYCH

REC
SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

Szczytniki 183
32-420 Gdów

Szczytniki, 2019

§1. Definicje

1. **Administrator danych osobowych (administrator danych)** – REC Spółka z ograniczoną odpowiedzialnością z siedzibą Szczytnikach pod adresem Szczytniki 183, 32-420 Gdów, wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego przez Sąd Rejonowy dla Krakowa-Śródmieścia w Krakowie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000453457, NIP: 6793090342, REGON: 122803262, kapitał zakładowy 20.000 zł.
2. **RODO** - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dn. 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.
3. **Ustawa** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.
4. **Urząd** – Prezes Urzędu Ochrony Danych Osobowych w Warszawie.
5. **Polityka** – niniejsza polityka bezpieczeństwa przetwarzania danych osobowych u Administratora danych osobowych.
6. **Dane osobowe** – wszelkie dane dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
7. **Zbiór danych** – posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
8. **Przetwarzanie danych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
9. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
10. **Inspektor Ochrony Danych (inspektor)** – osoba, o której mowa w art. 37 i nast. RODO, która z upoważnienia administratora danych zajmuje się w szczególności monitorowaniem przestrzegania u administratora zasad dotyczących przetwarzania danych oraz zgodnością przetwarzania z RODO i innymi właściwymi przepisami.
11. **Administrator Systemu Informatycznego (administrator systemu)** – osoba zarządzająca systemem informatycznym przetwarzającym dane osobowe.
12. **Użytkownik** – osoba fizyczna upoważniona przez administratora danych do przetwarzania danych osobowych, a zwłaszcza do przetwarzania danych w systemie informatycznym.
13. **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych w systemie informatycznym.

§2. Informacje ogólne

1. Niniejsza Polityka bezpieczeństwa przetwarzania danych osobowych została wprowadzona przez administratora danych na podstawie art. 24 ust. 2 RODO.
2. Polityka bezpieczeństwa wraz z Instrukcją zarządzania systemem informatycznym oraz Regulaminem ochrony danych osobowych stanowi kompletny opis systemu przetwarzania i ochrony danych osobowych wdrożony przez administratora danych.
3. Polityka bezpieczeństwa określa w szczególności zadania i obowiązki administratora danych oraz zasady ochrony i organizacji przetwarzania danych osobowych, w tym opis środków technicznych i organizacyjnych zastosowanych w celu zapewnienia przestrzegania zasad:

a) legalności – zapewnienie, iż dane osobowe są przetwarzane przez administratora danych zgodnie z prawem, na podstawie co najmniej jednej z przesłanek uprawniających do przetwarzania wskazanych w art. 6 ust. 1 lit. a-f RODO;
b) celowości - zapewnienie, iż dane osobowe są przetwarzane dla konkretnego, wyraźnego i prawnie uzasadnionego celu;
c) adekwatności – zapewnienie, iż dane osobowe przetwarzane są w takim zakresie, jaki niezbędny jest ze względu na cel ich przetwarzania;
d) merytorycznej poprawności – zapewnienie, iż administraotr danych ocenia wiarygodność źródła pozyskania danych poprzez wdrożenie sposobu weryfikowania prawdziwości przetwarzanych danych, a tym samym przetwarza dane poprawne i w razie potrzeby aktualizowane;
e) czasowości – zapewnienie, iż dane osobowe w formie umożliwiającej identyfikację osoby, której dotyczą, będą przetwarzane przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane zostały zebrane;
f) poufności - zapewnienie, iż dane nie są udostępniane nieupoważnionym podmiotom,
g) integralności – zapewnienie, iż zastosowano takie środki techniczne i organizacyjne, które chronią dane osobowe przed niedozwolonym przetwarzaneim oraz przed przypadkową utratą, zniszczeniem i uszkodzeniem;
h) rozliczalności – zapewnienie, iż działania podmiotu operującego danymi osobowymi mogą być jednoznacznie przypisane tylko temu podmiotowi, a podmiot przetwarzający dane jest w stanie wykazać, iż postępuje zgodnie z zasadami dotyczącymi przetwarzania danych osobowych;
i) przejrzystości – zapewnienie, iż osoby, których dane dotyczą otrzymują informacje związane z przetwarzaniem ich danych w formie łatwo dostepnej, w sposób zrozumiały oraz sformułowane jasnym i prostym językiem, a także zapewnienie, iż osoby upoważnione mają dostęp do informacji i zasobów z nią związanych wtedy, gdy jest to wymagane.

§3. Zakres stosowania

1. Politykę bezpieczeństwa stosuje się do danych przetwarzanych przez administratora danych jako własne zbiory danych osobowych, danych osobowych przetwarzanych jako współadministrator danych, jak i też w celu przetwarzania danych osobowych w związku z powierzeniem przetwarzania danych przez podmioty trzecie.
2. Do stosowania zasad określonych w Polityce bezpieczeństwa zobowiązany jest zarówno administrator danych jak, i osoby upoważnione przez administratora danych, a także inne osoby mające dostęp do danych osobowych podlegających ochronie. Administrator danych prowadzi ewidencję osób, które zostały zapoznane z niniejszym dokumentem.

§4. Administrator danych osobowych

1. Zadania administratora danych jako osoby prawnej wykonują członkowie organu uprawnionego do reprezentacji zgodnie z regulacjami Kodeksu spółek handlowych.
2. Do obowiązków administratora danych należą w szczególności:

a) wdrożenie odpowiednich środków technicznych i organizacyjnych adekwatnych do charakteru, zakresu, kontekstu i celu przetwarzania danych;
b) poddawanie okresowym przeglądom i uaktualnieniom środki, o których mowa w lit. a;
c) spełnienie obowiązku informacyjnego wobec osób, których dane osobowe będą przetwarzane;
d) przestrzeganie praw osób, których dane dotyczą, a to udzielanie dostępu do danych, sprostowanie, uaktualnienie, usuwanie danych oraz ograniczenie ich przetwarzania na żądanie osoby uprawnionej;
e) kontrola udostępniania i powierzania danych osobowych;
f) nadawanie upoważnień i prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
g) prowadzenie rejestru czynności przetwarzania danych osobowych zgodnie z art. 30 RODO.

3. Administrator danych może powołać Inspektora ochrony danych. W przypadkach określonych w art. 37 RODO powołanie inspektora jest obligatoryjne.
4. W przypadku niepowołania inspektora ochrony danych jego zadania wykonuje administrator danych.
5. Powołanie inspektora danych dokonywane jest zgodnie ze wzorem stanowiącym załącznik nr 10 (*Powołanie Inspektora Ochrony Danych)*.
6. Administrator danych dla zarzadzania systemem informatycznym może powołać Administratora Systemu Informatycznego.
7. W przypadku niepowołania Administratora Systemu Informatycznego jego zadania wykonuje administrator danych.

§5. Inspektor ochrony danych

1. Inspektor ochrony danych jest osobą posiadającą fachową wiedzę z zakresu ochrony danych osobowych, wyznaczoną przez administratora danych spośród własnego personelu lub z którą nawiązano współpracę na podstawie umowy o świadczenie usług do wykonywania zadań określonych w ust. 6.
2. Administrator danych zawiadamia Urząd o wyznaczeniu inspektora w terminie 14 dni od dnia jego wyznaczenia, wskazując imię, nazwisko, adres poczty elektronicznej i numer telefonu inspektora.
3. Inspektor jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań.
4. Inspektor podlega służbowo bezpośrednio najwyższemu kierownictwu administratora danych.
5. Administrator danych wspiera inspektora w wypełnianiu przez niego zadań, o których mowa w ust. 6, zapewniając mu zasoby niezbędne do wykonywania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.
6. Do zadań inspektora należy:
    a) informowanie administratora danych, podmiotu przetwarzającego, Administratora Systemu Informatycznego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na podstawie obowiązujących przepisów prawa dotyczących ochrony danych osobowych (w szczególności RODO oraz ustawy) i doradzanie w tym zakresie;
    b) monitorowanie przestrzegania obowiązujących przepisów prawa dotyczących ochrony danych osobowych (w szczególności RODO oraz ustawy) oraz

wdrożonych przez administraotra danych dokumentów składających się na system przetwarzania i danych osobowych (o którym mowa w §2 ust. 2);
   c) kontakt z osobami, których dane dotyczą;
   d) udzielnie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
   e) współpraca z Urzędem;
   f) pełnienie funkcji punktu kontaktowego dla Urzędu w kwestiach związanych z przetwarzaniem danych osobowych, w tym dla konsultacji, o których mowa w art. 36 RODO oraz konsultacji w innych wymagających tego sprawach.
7. Inspektor wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania danych.

§6. Osoby upoważnione (użytkownicy)

1. Osoby upoważnione przez administratora danych do przetwarzania danych osobowych zobowiązane są w szczególności do:
   a) przetwarzania danych osobowych tylko w zakresie udzielonego upoważnienia,
   b) przetwarzania danych osobowych tylko w celu, w którym zostały zgromadzone,
   c) przetwarzania i ochrony danych osobowych z zachowaniem zasady poufności,
   d) przestrzegania zasad ochrony danych osobowych określonych we wdrożonych przez administratora danych dokumentach składających się na system przetwarzania i danych osobowych (o którym mowa w §2 ust. 2) oraz wynikających z obowiązujących przepisów prawa (w szczególności RODO oraz ustawy),
   e) informowania administratora danych lub innej właściwej osoby, zgodnie z przyjętymi przez administratora danych zasadami, o wszelkich zdarzeniach związanych z naruszeniem bezpieczeństwa danych osobowych oraz naruszeniem zasad ochrony danych osobowych.
2. Upoważnienie do przetwarzania danych osobowych wydawane jest na piśmie zgodnie ze wzorem stanowiącym załącznik nr 1 (*Upoważnienie do przetwarzania danych osobowych).*
3. Administrator danych prowadzi rejestr osób upoważnionych do przetwarzania danych osobowych – załącznik nr 2 (*Rejestr upoważnień).*

§7. Zarządzanie incydentami

1. Przez *incydent* dotyczący danych osobowych uważa się w szczególności:
   a) naruszenie zasady dostępności – trwała ustrata lub zniszczenie danych osobowych,
   b) naruszenie zasady integralności – nieautoryzowana zmiana treści danych osobowych,
   c) naruszenie zasady poufności – ujawnienie danych osobowych nieuprawnionej osobie.
2. W przypadku stwierdzenia wystąpienia incydentu użytkownik jest zobowiązany do:
   a) gdy incydent zaistniał w systemie informatycznym - zablokowania dostępu do tego systemu,
   b) podjęcia działań mających na celu zminimalizowanie skutków incydentu lub całkowite wyeliminowanie zagrożenia,

c) zabezpieczenia dowodów umożliwiających ustalenie przyczyn oraz skutków incydentu,
d) powiadomienia, w przypadku administratora systemu informatycznego, gdy incydent dotyczy systemu informatycznego, a w innych przypadkach inspektora o incydencie, w tym określenia momentu jego wystąpienia (lub jego ujawnienia) oraz okoliczności jemu towarzyszących.

3. Administrator systemu informatycznego lub inspektor po otrzymaniu informacji o incydencie:
   a) ustali przyczyny i okoliczności naruszenia bezpieczeństwa przetwarzania danych osobowych,
   b) określi zakres danych osobowych, których dotyczył incydent,
   c) ustali osobę winną wystąpienia incydentu,
   d) określi skutki wystąpienia incydentu,
   e) ustali i podejmie działania w celu wyeliminowania skutków incydentu (działania korekcyjne) oraz działania w celu wyeliminowania przyczyn incydentu (działania korygujące),
   f) ustali i podejmie działania zapobiegające wystąpieniu podobnego incydentu w przyszłości (działania zapobiegawcze).
4. Po ujawnieniu incydentu administrator systemu informatycznego lub inspektor sporządzi raport z incydentu zgodnie z załącznikiem nr 4 (*Raport z incydentu naruszającego bezpieczeństwo danych osobowych)* oraz przedłoży sporządzony raport administratorowi danych.
5. Administrator danych po otrzymaniu raportu bez zbędnej zwłoki, nie później jednak, niż 72 godziny od wystąpienia incydentu, zgłosi incydent do Urzędu. W przypadku dokonania zgłoszenia po upływie 72 godzin, administrator danych dołącza do zgłoszenia pisemne wyjasnienie opóźnienia.
6. Administrator danych nie jest zobowiązany do zgłoszenia incydentu w przypadku, gdy mało prawdopodobnym jest, iż naruszenie będzie skutkować naruszeniem praw lub wolności osób, których dane dotyczą.
7. Administrator danych dokonuje zgłoszenia do Urzędu z zastosowaniem formularza stanowiącego załącznik nr 6 (*Formularz zgłoszenia incydentu).*
8. W przypadku gdy incydent może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator danych bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
9. Zawiadomienie, o którym mowa w ust. 8 powinno być sformułowane jasnym i prostym językiem, opisywać charakter naruszenia ochrony danych osobowych oraz zawierać co najmniej:
   a) zawierać dane inspektora (imię i nazwisko) oraz dane kontaktowe, a w przypadku jego niepowołania, dane kontaktowe do innej osoby, od której można uzyskać bliższe informacje,
   b) opisywać możliwe konsekwencje naruszenia ochrony danych,
   c) opisywać działania korekcyjne oraz korygujące podjęte przez administratora danych.

§8. Dane osobowe

1. Administrator danych przetwarza dane osobowe w celu świadczenia usług leżących w zakresie jego działalności gospodarczej, a także w celach rachunkowych oraz w celach kadrowych.
2. Administrator danych przetwarza dane zarówno w formie papierowej (tradycyjnej) jak i formie elektronicznej.

3. Dane osobowe przetwarzane przez administratora danych uzyskiwane są bezpośrednio od osoby, której dotyczą. Dopuszczalne jest pozyskiwanie danych osobowych z innego źródła, jeżeli jest to dozwolone na podstawie obowiązujących przepisów prawa.
4. 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 danych podejmie czynności, o których mowa w art. 35 i nast. RODO.
5. W przypadku planowania nowych czynności przetwarzania danych, administrator danych dokonuje analizy ich skutków dla ochrony danych osobowych oraz uwzględnia kwestie ochrony danych osobowych w fazie ich projektowania.

§9. Rejestr czynności przetwarzania danych osobowych

1. Administrator danych prowadzi rejestr czynności przetwarzania danych osobowych (rejestr), o którym mowa w art. 30 RODO.
2. Rejestr prowadzony przez administratora danch dokumentuje czynności przetwarzania danych, określając m. in. cel przetwarzania danych, kategorie danych oraz osób, których dane dotyczą oraz podstawy prawne przetwarzania, a tym samym stanowi narzędzie służące wywiązaniu się z zasady rozliczalności wskazanej w §2 ust. 3 lit. h.
3. Rejestr stanowi załącznik nr 3 do niniejszej Polityki bezpieczeństwa.
4. Rejestr prowadzony jest w formie elektronicznej umożliwiającej jego wydruk i nastepnie prowadzenie w formie papierowej.

§10. Środki techniczne i organizacyjne

W celu ochrony przetwarzania danych osobowych podjęto następujące działania:

a) zapewniono odpowiednie do zagrożeń i kategorii przetwarzania danych objętych ochroną środki techniczne i organizacyjne,
b) prowadzony jest rejestr osób upoważnionych (użytkowników) do przetwarzania danych osobowych,
c) opracowano i wdrożono Politykę bezpieczeństwa przetwarzania danych osobowych,
d) opracowano i wdrożono Instrukcję zarządzania systemem informatycznym,
e) opracowano i wdrożono Regulamin ochrony danych,
f) zapoznano osoby upoważnione do przetwarzania danych osobowych z aktualnie obowiązującymi przepisami prawa dotyczącymi danych osobowych oraz z treścią Polityki bezpieczeństwa, Instrukcji zarzadzania systemem informatycznym oraz Regulaminem ochrony danych.

§11. Powierzenie przetwarzania danych osobowych

1. Administrator danych, w myśl art. 28 RODO może powierzyć przetwarzanie danych innemu podmiotowi.
2. Powierzenie przetwarzania danych osobowych powinno nastapić tylko takiemu podmiotowi, który zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi obowiązujących przepisów prawa dotyczących ochrony danych osobowych (w szczególności RODO oraz ustawy) i chroniło prawa osób, których dane dotyczą.

3. Powierzenie przetwarzania danych osobowych nastepuje na podstawie pisemnej umowy, której wzór stanowi załącznik nr 7 do niniejszego dokumentu (*Umowa powierzenia przetwarzania danych osobowych).* Powierzenie przetwarzania danych osobowych może nastapić na podstawie innego wzrou umowy, jeżeli spełnia on co najmniej wymagania nałozone przez art. 28 ust. 3 RODO.
4. Podmiot, któremu administrator danych powierzył przetwarzanie danych osobowych, może przetwarzać dane wyłącznie w zakresie i w celu przewidzianym w umowie.
5. Wykaz podmiotów, którym administrator danych powierzył przetwarzanie danych stanowi załącznik nr 8 (*Wykaz podmiotów, którym powierzono przetwarzanie danych).*

§12. Udostępnianie danych osobowych

1. Administrator danych udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
2. Dane osobowe mogą być udostępniane w następujących przypadkach:
    a) na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów;
    b) na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych;
    c) na podstawie wniosku osoby, której dane dotyczą.
3. Wniosek o udostępnienie danych osobowych powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie. Wzór wniosku stanowi załącznik nr 9 (*Wniosek o udostępnienie danych osobowych)*.
4. Udostępniając dane osobowe, należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
5. W przypadku żądania udzielenia informacji na temat przetwarzanych danych osobowych na pisemny wniosek pochodzący od osoby, której dane dotyczą, odpowiedź na wniosek następuje w terminie 30 dni od daty jego otrzymania.
6. Wniosek o udostępnienie przekazywany jest do administratora danych.
7. Administrator danych może odmówić udostępnienia danych osobowych. Odmowa udostępnienia danych osobowych następuje wówczas, gdy spowodowałoby to istotne naruszenia dóbr osobistych osób, których dane dotyczą lub innych osób oraz jeżeli dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania wnioskodawcy.

§13. Obowiązki informacyjne

1. Administrator danych wypełnia obowiązki informacyjne względem osób, których dane dotyczą.
2. W przypadku pozyskiwania danych osobowych bezpośrednio od osoby, której one dotyczą, administrator danych spełnia obowiązki informacyjne przy pozyskiwaniu danych.
3. W przypadku pozyskiwania danych osobowych od innego podmiotu, niż osoba, której one dotyczą, administrator danych niezwłocznie spełnia obowiązek informacyjny wobec osoby, której dane dotyczą.
4. W przypadku przetwarzania danych, za pomocą których nie można zidentyfikować konkretnej osoby fizycznej, administrator danych spełnia obowiązki informacyjne poprzez zamieszczenie stosownych informacji w miejscu prowadzenia działalności gospodarczej oraz na należących do niego stronach internetowych.

5. Spełnienie obowiązków informacyjnych następuje poprzez przekazanie osobie, której dane dotyczą informacji, o których mowa w art. 13 oraz 14 RODO.

§14. Postanowienia końcowe

1. Polityka bezpieczeństwa przetwarzania danych osobowych stanowi tajemnicę przedsiębiorstwa administratora danych i jako taka podlega ochronie przewidzianej przepisami prawa.
2. Zapoznanie się i wdrożenie postanowień Polityki bezpieczeństwa stanowi obowiązek każdej osoby dopuszczonej do przetwarzania danych w przedsiębiorstwie administratora danych.
3. Polityka bezpieczeństwa obowiązuje od dnia jej zatwierdzenia przez administratora danych.
4. Zmiana treści załączników nie stanowi zmiany Polityki bezpieczeństwa, a tym samym nie wymaga jej ponownego zatwierdzenia przez administratora danych.

Lista załączników:
Załącznik nr 1 – Upoważnienie do przetwarzania danych osobowych
Załącznik nr 2 – Rejestr upoważnień
Załącznik nr 3 – Rejestr czynności przetwarzania danych osobowych
Załącznik nr 4 – Raport z incydentu
Załącznik nr 5 – Rejestr incydentów
Załącznik nr 6 – Wzór zgłoszenia incydentu
Załącznik nr 7 – Wzór umowy powierzenia przetwarzania danych osobowych
Załącznik nr 8 – Wykaz podmiotów, którym powierzono przetwarzanie danych osobowych
Załącznik nr 9 – Wniosek o udostepnienie danych osobowych
Załącznik nr 10 – Powołanie Inspektora Ochrony Danych

_____ (data zatwierdzenia)

_____ (w imieniu administratora danych)

Załącznik nr 1

Miejscowość, dnia _____ r.

_____
(pieczęć administratora danych)

UPOWAŻNIENIE
do przetwarzania danych osobowych

Z dniem _____ na podstawie art. 37 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dn. 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 (RODO) upoważniam Pana/Panią

_____

do przetwarzania danych osobowych w zakresie:

_____

(nazwa zbioru danych osobowych)

Upoważnienie obejmuje:

☐ dane osobowe przetwarzane w formie papierowej
☐ dane osobowe przetwarzane w systemie informatycznym

Upoważnienie obejmuje przetwarzanie danych:

☐ bez ograniczeń
☐ podgląd danych
☐ wprowadzanie danych
☐ edycja danych

Równocześnie zobowiązuję Pana/Panią do przestrzegania przepisów dotyczących ochrony danych osobowych określonych przepisami RODO, ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych oraz postanowień dokumentacji wdrożonej przez administratora danych (*Polityka bezpieczeństwa przetwarzania danych osobowych, Instrukcja zarządzania systemem informatycznym oraz Regulamin ochrony danych*).

Niniejsze upoważnienie obowiązuje od dnia _____ do odwołania.

_____
(podpis upoważniającego)

OŚWIADCZENIE

Oświadczam, iż zapoznałem/am się z przepisami dotyczącymi ochrony danych osobowych oraz wdrożonymi przez administratora danych dokumentami, w szczególności *Polityką bezpieczeństwa przetwarzania danych osobowych, Instrukcją zarządzania systemem informatycznym oraz Regulaminem ochrony danych.*
Oświadczam ponadto, iż zobowiązuję się do:

a) zachowania w tajemnicy danych osobowych, do których uzyskałem dostęp w związku ze stosunkiem pracy lub wykonywaniem zobowiązań umownych u administratora danych,
b) niewykorzystywania danych osobowych do celów innych, niż te co do których zostały zgromadzone przez administratora danych,
c) zachowania w tajemnicy metod i zasad zabezpieczania danych osobowych u administratora danych,
d) korzystania wyłącznie z oprogramowania i sprzętu dostarczonego przez administratora danych,
e) należytej dbałości o oprogramowanie i sprzęt administratora danych.

Oświadczam, iż w przypadku niestosowania się do powyższych zobowiązań, jestem świadomy/a odpowiedzialności pracowniczej lub odpowiedzialności wynikającej ze zobowiązań umownych, a także odpowiedzialności karnej w przypadku naruszenia przepisów RODO lub ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

_____
(podpis upoważnionego)

Załącznik nr 2

REJESTR UPOWAŻNIEŃ

Lp.	Imię i nazwisko	Identyfikator w systemie informatycznym	Zbiór danych objęty upoważnieniem	Data nadania upoważnienia	Data wygaśnięcia upoważnienia
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					
15.					

Załącznik nr 4

Nr raportu: _____

RAPORT
z incydentu naruszającego bezpieczeństwo danych osobowych

I

Sporządzający raport	
Imię i nazwisko	
Funkcja	

II

Miejsce i czas wystąpienia incydentu	
Miejsce (piętro, pokój, urządzenie)	
Data	
Godzina	

III

Osoby powodujące naruszenie (zarówno przez działanie jak i zaniechanie)		
1.	**Imię i nazwisko**	
	Funkcja	
2.	**Imię i nazwisko**	
	Funkcja	
3.	**Imię i nazwisko**	
	Funkcja	

IV

Osoby uczestniczące w zdarzeniu związanym z incydentem		
1.	**Imię i nazwisko**	
	Funkcja	
2.	**Imię i nazwisko**	
	Funkcja	
3.	**Imię i nazwisko**	
	Funkcja	

V

Informacje o danych, które zostały lub mogły zostać ujawnione		
Nazwa zbioru danych	**Zakres danych**	**Program/system służący do przetwarzania**

VI

Zabezpieczone materiały lub inne dowody związane z incydentem	
1.	
2.	
3.	
4.	
5.	
6.	

VII

Krótki opis wydarzenia związanego z naruszeniem ochrony danych osobowych (przebieg zdarzenia, opis zachowania uczestników, podjęte działania korekcyjne, korygujące oraz zapobiegawcze)

Podpis sporządzającego raport: **Data:**

Załącznik nr 5

REJESTR INCYDENTÓW

Nr raportu	Osoba		Podjęte działania (zaznaczyć właściwe „x”)			Data ustania zagrożenia	Uwagi
	zgłaszająca	powodująca naruszenie	korekcyjne	korygujące	zapobiegawcze		

Załącznik nr 6

----------,---------- r.

(miejscowość , data)

REC Sp. z o.o.
Szczytniki 183, 32-420 Gdów
REGON: 122803262

Prezes Urzędu Ochrony Danych Osobowych
ul. Stawki 2
00-193 Warszawa

ZGŁOSZENIE
incydentu naruszenia ochrony danych osobowych

Niniejszym, w trybie art. 33 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dn. 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*, zgłaszam naruszenie ochrony danych osobowych:

Miejsce i data incydentu	
Charakter naruszenia ochrony danych	
Kategoria i przybliżona liczba osób, których dane dotyczą	
Kategorie i przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie	
Możliwe konsekwencje naruszenia ochrony danych	
Środki zastosowane w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych	

(uzasadnienie zwłoki, gdy zgłoszenie dokonane po upływie 72 godzin od stwierdzenia naruszenia)

(podpis w imieniu administratora danych)

Załącznik nr 7

UMOWA
powierzenia przetwarzania danych osobowych

zawarta dnia _____ w Białymstoku pomiędzy:

REC Spółką z ograniczoną odpowiedzialnością z siedzibą Szczytnikach pod adresem Szczytniki 183, 32-420 Gdów, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego przez Sąd Rejonowy dla Krakowa-Śródmieścia w Krakowie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000453457, NIP: 6793090342, REGON: 122803262, kapitał zakładowy 20.000 zł, zwaną dalej **„Administratorem danych”**,
reprezentowaną przez _____ ,

a

Nazwa	
Adres	
NIP	
Osoba reprezentująca	

dalej **„Przetwarzającym”**,

o następującej treści:

§1

1. Strony zawarły w dniu _____ umowę w przedmiocie _____ .
2. Na podstawie umowy, o której mowa w ust. 1, Przetwarzający będzie miał możliwość dostępu do danych osobowych przetwarzanych przez Administratora.

§2

1. Administrator jest administratorem danych osobowych w rozumieniu art. 4 pkt 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dn. 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 (dalej RODO).
2. Administrator w trybie art. 28 RODO powierza przetwarzanie danych osobowych Przetwarzającemu na zasadach, w celu i w zakresie określonym niniejszą umową.
3. Przetwarzający oświadcza, że przekazane dane osobowe będą przetwarzane wyłącznie na zasadach, w zakresie i celu określonym w umowie.
4. Dane osobowe będą przetwarzane przez Przetwarzającego wyłącznie w celu realizacji umowy, o której mowa w §1. Poprzez przetwarzanie danych rozumie się wyłącznie: *zbieranie, zapisywanie, modyfikację, przesyłanie, przechowywanie oraz utrwalanie danych (zostawiamy tylko czynności, które będą faktycznie wykonywane przez Przetwarzającego)*.

5. Dane osobowe będą przetwarzane w następującym zakresie: *(wymieniamy dane osobowe jakie będą powierzone „Przetwarzającemu" np. imię i nazwisko, adres zamieszkania)*.

§3

1. Przetwarzający zobowiązuje się do zastosowania przy przetwarzaniu danych osobowych wszelkich środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych zgodnie z art. 32 RODO.
2. W szczególności Przetwarzający jest zobowiązany do:
   a) nadzorowania przestrzegania zasad ochrony przetwarzanych danych osobowych;
   b) zabezpieczenia przetwarzanych danych osobowych przed: udostępnieniem osobie nieupoważnionej, przetwarzaniem z naruszeniem postanowień umowy lub zmianą, utratą, uszkodzeniem bądź zniszczeniem;
   c) posiadania odpowiednich procedur opisujących sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne stosowane w celu zapewnienia ochrony przetwarzanych danych osobowych;
   d) zapewnienia, aby do przetwarzania danych były dopuszczone jedynie osoby posiadające upoważnienie nadane im przez Przetwarzającego oraz prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych;
   e) zapewnienia zachowania w tajemnicy przetwarzanych danych osobowych, w szczególności poprzez zobowiązanie osób upoważnionych do przetwarzania danych osobowych do zachowania poufności.

§4

1. Przetwarzający jest odpowiedzialny za przetwarzanie danych niezgodne z umową lub zasadami określonymi przez RODO.
2. Przetwarzający zobowiązuje się do niezwłocznego poinformowania administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania powierzonych danych osobowych.
3. Przetwarzający w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz pomaga wywiązać się z obowiązków określonych w art. 32-36 RODO.
4. Przetwarzający ponosi pełną odpowiedzialność za naruszenia zasad przetwarzania i ochrony danych osobowych przez podmiot, któremu powierzył dalsze przetwarzanie danych.
5. Przetwarzający udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych niniejszą umową oraz zasadami określonymi przez RODO oraz umożliwia administratorowi przeprowadzanie audytów, w tym inspekcji i przyczyniania się do nich o czym mowa w art. 28 ust. 3 lit. h RODO.

§5

1. Przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania jedynie za wyraźną zgodą administratora wyrażona na piśmie lub za pośrednictwem poczty elektronicznej.
2. Podmiot, któremu powierzający przekazał dane do dalszego przetwarzania, zobowiązany jest do wypełnienia takich samych obowiązków jak te nałożone na przetwarzającego niniejszą umową i zasadami określonymi przez RODO.

§6

1. Niniejsza umowa zostaje zawarta na czas określony zgodnie z terminem, na jaki została zawarta umowa, o której mowa w §1.
2. Przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem danych, zależnie od decyzji administratora, usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie istniejące kopie danych, chyba że szczególne przepisy prawa zobowiązują przetwarzającego do przechowywania danych.
3. Przetwarzający zobowiązuje się niezwłocznie powiadomić Administratora, że czynności, o których mowa w ust. 2 zostały wykonane, a w razie ich niewykonania o przyczynach niewykonania.

§7

1. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.
2. W zakresie nieuregulowanym przez umowę zastosowanie mają przepisy RODO oraz innych odpowiednich aktów prawnych.
3. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

_____ _____

(w imieniu Administratora) (w imieniu Przetwarzającego)

Załącznik nr 8

WYKAZ PODMIOTÓW, KTÓRYM POWIERZONO PRZETWARZANIE DANYCH OSOBOWYCH

Lp.	Nazwa oraz siedziba podmiotu	Data powierzenia	Kategoria osób, których dane dotyczą	Cel powierzenia
1.				
2.				
3.				
4.				
5.				
6.				

Załącznik nr 9

Wniosek o udostępnienie danych osobowych

1. Wniosek do

_____

_____
(dokładna nazwa administratora danych)

2. Wnioskodawca

_____

_____

_____
(nazwa firmy/imię i nazwisko, adres siedziby/zamieszkania, NIP, REGON, dane do korespondencji)

3. Podstawa prawna upoważniająca wnioskodawcę do przetwarzania danych osobowych jako odbiorcy danych:

1) _____

2) _____

3) _____

4) _____

4. Cel przetwarzania danych:

1) _____

2) _____

3) _____

5. Nazwa zbioru, z którego mają być udostępnione dane osobowe lub informacje umożliwiające zidentyfikowanie dokumentów, w których występowały dane osobowe:

1) _____

2) _____

3) _____

6. Zakres wymaganych danych, jakie mają być udostępnione:

1) _____

2) _____
3) _____

4) _____

7. Forma doręczenia udostępnianych danych osobowych:

_____

_____

8. Lista załączników do wniosku:

1) _____

2) _____

3) _____

_____

(miejscowość, data i podpis osoby wnioskującej lub upoważnionej przez wnioskodawcę)

Wypełnia administrator danych	
Decyzja administratora danych	Wyrażam zgodę / nie wyrażam zgody* na udostepnienie danych. (niepotrzebne skreślić)
Data udostępnienia danych	
Nazwa zbioru, z którego udostępniono dane	
Zakres udostępnionych danych	

Załącznik nr 10

POWOŁANIE

INSPEKTORA OCHRONY DANYCH

Niniejszym powołuję _____

(imię i nazwisko)

PESEL: _____, do pełnienia funkcji Inspektora Ochrony Danych w:

REC Sp. z o.o.

Szczytniki 183
32-420 Gdów

W drodze niniejszego powołania Inspektor Ochrony Danych zobowiązany jest do wykonywania obowiązków określonych *Polityką Bezpieczeństwa Przetwarzania Danych Osobowych* oraz *Instrukcją Zarządzania Systemem Informatycznych* w celu zapewnienia zgodności przetwarzania danych z wdrożoną przez administratora danych dokumentacją oraz powszechnie obowiązującymi przepisami prawa w zakresie ochrony danych osobowych tj. rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dn. 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* oraz innych właściwych przepsiów prawa.

_____ _____

(data, podpis administratora danych) (podpis inspektora ochrony danych)