POLITYKA
OCHRONY DANYCH OSOBOWYCH

COLOREX SYSTEM
SP. Z O.O.

Kraków, dnia 31.08.2019 r.

Niniejszy dokument zatytułowany *Polityka Ochrony Danych Osobowych* zwana dalej „Polityką", został sporządzony w celu wykazania, że w **COLOREX SYSTEM sp. z o.o.** (dalej jako: „Administrator Danych" lub „Jednostka") dane osobowe są przetwarzane i zabezpieczone zgodnie z wymogami prawa, dotyczącymi zasad przetwarzania i zabezpieczenia danych, w tym zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 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") oraz ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.

Definicje:

1. **Administrator Danych –** COLOREX SYSTEM spółka z ograniczoną odpowiedzialnością z siedzibą w Krakowie, ul. Łuczanowicka 30, 31-766 Kraków (zakład – ul. Ujastek 1 w Krakowie), wpisana do Rejestru Przedsiębiorców - Krajowego Rejestru Sądowego w Sądzie Rejonowym dla Krakowa-Śródmieścia w Krakowie XI Wydziale Gospodarczym KRS pod numerem KRS 0000018559, o kapitale zakładowym w wysokości 50.000,00 PLN, NIP 6782825194, REGON 356303549;
2. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
3. **Dane szczególnych kategorii** – oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej;
4. **Podmiot przetwarzający** – oznacza organizację lub osobę, której Administrator Danych powierzył przetwarzanie danych osobowych (np. tłumacz, zewnętrzna księgowość, zewnętrzna firma kurierska etc.);
5. **Profilowanie** – oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystywaniu 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;
6. **Eksport danych** – oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej;
7. **IOD lub Inspektor** – oznacza Inspektora Ochrony Danych Osobowych;
8. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu Przetwarzania danych;
9. **Użytkownik** – osoba upoważniona przez Administratora Danych do Przetwarzania danych osobowych;
10. **Zbiór danych** – każdy uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów;
11. **Przetwarzanie danych** – jakiekolwiek operacje wykonywane na Danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwa-

nie w formie tradycyjnej oraz w systemach informatycznych, w szczególności przetwarzanie danych związane z realizacją usługi telemarketingu;

12. **Rejestr** – oznacza Rejestr Czynności Przetwarzania Danych Osobowych;
13. **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym (Użytkownika) w razie Przetwarzania danych osobowych w takim systemie**;**
14. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym (Użytkownikowi) w razie przetwarzania danych osobowych w takim systemie;
15. **RODO** – oznacza Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 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;
16. **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu (Użytkownika).

Postanowienia ogólne

1. Polityka dotyczy wszystkich Danych osobowych przetwarzanych w przedsiębiorstwie Administratora, niezależnie od formy ich przetwarzania (w formie tradycyjnej i w Systemach informatycznych) oraz od tego, czy dane są lub mogą być przetwarzane w Zbiorach danych.
2. Polityka jest przechowywana w wersji elektronicznej oraz/lub w wersji papierowej w siedzibie Administratora Danych lub w zakładzie przy ul. Ujastek 1 w Krakowie.
3. Polityka jest udostępniana do wglądu osobom posiadającym upoważnienie do przetwarzania danych osobowych na ich wniosek, a także osobom, którym ma zostać nadane upoważnienie do przetwarzania danych osobowych, celem zapoznania się z jej treścią oraz osobom, z którymi Administrator Danych zawarł umowy powierzenia danych osobowych do przetwarzania.
4. Dla skutecznej realizacji Polityki Administrator Danych zapewnia:
   a) środki techniczne i rozwiązania organizacyjne odpowiednie do zagrożeń i kategorii danych objętych ochroną,
   b) kontrolę i nadzór nad Przetwarzaniem danych osobowych,
   c) monitorowanie zastosowanych środków ochrony.
5. 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.
6. Administrator Danych zapewnia, że czynności wykonywane w związku z przetwarzaniem i zabezpieczeniem danych osobowych są zgodne z Polityką oraz odpowiednimi przepisami prawa.
7. Polityka zawiera:
   a) opis zasad ochrony danych obowiązujących w Jednostce;
   b) uszczegóławiające odwołania do załączników (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach).

8. Za nadzór i monitorowanie przestrzegania Polityki odpowiadają:
   a) Komórka audytu wewnętrznego, jeżeli funkcjonuje w Jednostce (powoływana w wyjątkowych przypadkach zidentyfikowania zagrożeń).
   b) Administrator Danych.
9. Za stosowanie Polityki odpowiedzialni są:
   a) Administrator Danych,
   b) wszyscy pracownicy i współpracownicy Administratora Danych.

I. Ochrona danych osobowych u Administratora Danych – zasady ogólne

1. Filarami ochrony danych osobowych są:
   a) **Legalność –** Administrator Danych dba o ochronę prywatności i przetwarza dane zgodnie z prawem;
   b) **Bezpieczeństwo –** Administrator Danych zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stale działania w tym zakresie;
   c) **Prawa jednostki –** Administrator Danych umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje;
   d) **Rozliczalność –** Administrator Danych dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność Przetwarzania z wymogami prawa wynikającymi z RODO i innych przepisów dotyczących ochrony danych osobowych.
2. Administrator Danych dba o minimalizację przetwarzania danych pod kątem:
   a) adekwatności danych do celów (ilości danych i zakresu przetwarzania),
   b) dostępu do danych,
   c) czasu przechowywania danych.
3. Administrator Danych przetwarza dane osobowe z poszanowaniem następujących zasad:
   a) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
   b) rzetelnie i uczciwie (rzetelność);
   c) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
   d) w konkretnych celach (minimalizacja);
   e) nie więcej niż potrzeba (adekwatność);
   f) z dbałością o prawidłowość danych (prawidłowość);
   g) nie dłużej niż potrzeba (czasowość);
   h) zapewniając odpowiednie bezpieczeństwo (bezpieczeństwo).
4. Administrator Danych spełnia obowiązki informacyjne względem osób, których dane przetwarza oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:

a) **obowiązki informacyjne –** przy zbieraniu danych i w innych sytuacjach Administrator Danych przekazuje osobom wymagane prawem informacje oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków;

b) **możliwość wykonania żądań –** Administrator Danych weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających;

c) **obsługa żądań –** Administrator Danych zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany przez RODO oraz aby były udokumentowane;

d) **zawiadomienie o naruszeniach –** Administrator Danych stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

5. Administrator Danych identyfikuje przypadki, w których przetwarza lub może przetwarzać dane szczególnych kategorii lub dane karne oraz utrzymuje mechanizmy zapewnienia zgodności z prawem przetwarzania takich danych. W przypadku zidentyfikowania przypadków przetwarzania danych szczególnych kategorii lub danych karnych Jednostka postępuje zgodnie z przyjętymi zasadami w tym zakresie, określonymi w RODO i innych przepisach dotyczących ochrony danych osobowych.
6. Administrator Danych identyfikuje przypadki, w których dokonuje profilowania przetwarzanych danych i utrzymuje mechanizmy zapewniające zgodność tego procesu z prawem. W przypadku zidentyfikowania przypadków profilowania i zautomatyzowanego podejmowania decyzji Jednostka postępuje zgodnie z przyjętymi zasadami w tym zakresie, określonymi w RODO i innych przepisach dotyczących ochrony danych osobowych.
7. Administrator Danych identyfikuje przypadki współadministrowania danymi. W przypadku zidentyfikowania postępuje w tym zakresie zgodnie z przyjętymi zasadami, określonymi w RODO i innych przepisach dotyczących ochrony danych osobowych.

II. Dane osobowe przetwarzane u Administratora Danych

1. Dane osobowe przetwarzane przez Administratora Danych gromadzone są w zbiorach danych.
2. Administrator Danych nie podejmuje czynności przetwarzania, które mogłyby się wiązać z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka dla praw i wolności osób, których dane są przetwarzane. W przypadku planowania takiego działania Administrator Danych wykona czynności określone w art. 35 i nast. RODO (ocena skutków dla ochrony danych).
3. W przypadku planowania nowych czynności przetwarzania Administrator dokonuje analizy ich skutków dla ochrony danych osobowych oraz uwzględnia kwestie ochrony danych w fazie ich projektowania (*„data protection by design”*).
4. Administrator Danych dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.
5. Administrator Danych wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw osoby i obowiązków informacyjnych.

6. W celu realizacji praw osoby Administrator Danych zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzanych przez Jednostkę, zignorować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany.
7. Administrator Danych określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.
8. Administrator Danych informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.
9. Administrator Danych informuje osobę o przetwarzaniu jej danych, jeśli pozyskuje dane nie od tej osoby.
10. Administrator Danych bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

III. Żądania osób

1. **Prawa osób trzecich.** Realizując prawa osób, których dane dotyczą Jednostka wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej informacji o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnicę handlową, dobra osobiste). Administrator Danych może się zwrócić do osoby kierującej żądanie w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową spełniania żądania.
2. **Nieprzetwarzanie.** Administrator Danych informuję osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.
3. **Odmowa.** Administrator Danych informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych. Administrator Danych informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.
4. **Dostęp do danych.** Na żądanie osoby dotyczące dostępu do jej danych Administrator Danych informuje osobę, czy przetwarza jej dane, oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych, z zastrzeżeniem, że kopii danych wydanej w wykonaniu prawa dostępu do danych Administrator Danych nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych (patrz pkt 5 poniżej).
5. **Kopie danych.** Na żądanie Administrator Danych wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Za kolejne kopie Administrator Danych może pobierać opłaty, gdzie cena takiej kopii danych skalkulowana będzie na podstawie oszacowanego jednostkowego kosztu obsługi wydania kopii danych.
6. **Sprostowanie danych.** Administrator Danych dokonuje na żądanie osoby sprostowania nieprawidłowych danych. Administrator Danych ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Administrator Danych na żądanie tej osoby informuje osobę o odbiorcach danych.

7. **Uzupełnienie danych.** Administrator Danych uzupełnia i aktualizuje dane na żądanie osoby. Administrator Danych ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. Administrator Danych nie musi przetwarzać danych, które są dla niego zbędne).
8. **Usunięcie danych.** Na żądanie osoby Administrator Danych usuwa dane, gdy:
   a) dane nie są niezbędne do celów, w których zostały zebrane, ani nie są przetwarzane w innych zgodnych z prawem;
   b) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania;
   c) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych;
   d) dane były przetwarzane niezgodnie z prawem;
   e) konieczność usunięcia wynika z obowiązku prawnego;
   f) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. profil dziecka na portalu społecznościowym, udział w konkursie).

   Administrator Danych określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17 ust. 3 RODO. W przypadku usunięcia danych Administrator Danych informuje osobę o odbiorcach danych, na żądanie tej osoby.
9. **Ograniczenie przetwarzania.** Administrator Danych dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:
   a) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość;
   b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
   c) Administrator Danych nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
   d) Osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Administratora Danych zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

   W trakcie ograniczenia przetwarzania Administrator Danych przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu obrony praw innej osoby fizycznej lub prawnej lub z uwagi na ważne względy interesu publicznego. Administrator Danych informuje osobę przed uchyleniem ograniczenia przetwarzania. W przypadku ograniczenia przetwarzania danych Administrator Danych na żądanie tej osoby informuje osobę o odbiorcach danych.
10. **Przenoszenie danych.** Na żądanie osoby Administrator Danych wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Administratorowi Danych, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania zawartej z nią umowy.

11. **Sprzeciw w szczególnej sytuacji.** Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Administratora Danych w oparciu o uzasadniony interes Administratora Danych lub o powierzone Administratorowi Danych zadanie w interesie publicznym, Administrator Danych uwzględni sprzeciw, o ile nie zachodzą po jego stronie ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.
12. **Sprzeciw względem marketingu bezpośredniego.** Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Administratora Danych na potrzeby marketingu bezpośredniego (w tym ewentualnie profilowania), Administrator Danych uwzględni sprzeciw i zaprzestanie takiego przetwarzania.
13. **Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu.** Jeżeli Administrator Danych przetwarza dane w sposób automatyczny, w tym w szczególności profiluje osoby, i w konsekwencji podejmuje względem osoby decyzje wywołujące skutki prawne lub inaczej istotnie wpływające na osobę, Administrator Danych zapewnia możliwość odwołania się do interwencji i decyzji człowieka po stronie Administrator Danych, chyba że taka automatyczna decyzja:
    a) jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a Administratorem Danych, lub
    b) jest wprost dozwolona przepisami prawa, lub
    c) opiera się na wyraźnej zgodzie odwołującej osoby.

IV. Rejestr Czynności Przetwarzania Danych

1. Administrator danych opracowuje, prowadzi i utrzymuje Rejestr.
2. Wzór Rejestru stanowi **Załącznik nr 1** do Polityki.
3. Rejestr stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.
4. Administrator Danych prowadzi Rejestr, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.
5. W Rejestrze dla każdej odrębnej czynności przetwarzania danych odnotowuje:
    a) nazwę czynności;
    b) cel przetwarzania;
    c) opis kategorii osób;
    d) opis kategorii danych;
    e) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu Administratora Danych, jeżeli podstawą jest uzasadniony interes;
    f) sposób zbierania danych;
    g) opis kategorii odbiorców danych (w tym przetwarzających)
    h) informację o przekazaniu poza EU/EUG;

i) opis technicznych i i organizacyjnych środków ochrony danych.

6. Administrator Danych dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności.

V. Obowiązki i odpowiedzialność w zakresie zarządzania bezpieczeństwem

1. Wszystkie osoby zobowiązane są do przetwarzania danych osobowych zgodnie z obowiązującymi przepisami i zgodnie z ustaloną przez Administratora Danych Polityką Ochrony Danych Osobowych, Instrukcją Zarządzania Systemem Informatycznym, a także innymi dokumentami wewnętrznymi i procedurami związanymi z Przetwarzaniem danych osobowych obowiązującymi u Administratora Danych.
2. Wszystkie Dane osobowe u Administratora Danych są przetwarzane z poszanowaniem zasad przetwarzania przewidzianych przez przepisy prawa:
   a) w każdym wypadku występuje chociaż jedna podstawa prawna dla przetwarzania danych przewidziana przepisami prawa;
   b) dane są przetwarzane rzetelnie i w sposób przejrzysty;
   c) dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
   d) Dane osobowe są przetwarzane jedynie w takim zakresie, jaki jest niezbędny dla osiągnięcia celu przetwarzania danych;
   e) dane osobowe są prawidłowe i w razie potrzeby uaktualniane;
   f) czas przechowywania danych jest ograniczony do okresu ich przydatności do celów, do których zostały zebrane, a po tym okresie są one usuwane;
   g) wobec osoby, której dane dotyczą, wykonywany jest obowiązek informacyjny zgodnie z treścią art. 13 i 14 RODO;
   h) dane są zabezpieczone przed naruszeniami zasad ich ochrony w Instrukcji zarządzania systemem informatycznym.
3. Administrator danych nie przekazuje osobom, których dane dotyczą, informacji, gdy zachodzi co najmniej jedna z sytuacji opisanej w art. 14 ust. 5 RODO.
4. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony Danych osobowych uważa się w szczególności:
   a) naruszenie bezpieczeństwa Systemów informatycznych, w których przetwarzane są dane osobowe, w razie ich przetwarzania w takich systemach;
   b) udostępnianie lub umożliwienie udostępniania danych osobom lub podmiotom do tego nieupoważnionym;
   c) zaniechanie, choćby nieumyślne, dopełnienia obowiązku zapewnienia danym osobowym ochrony;
   d) niedopełnienie obowiązku zachowania w tajemnicy Danych osobowych oraz sposobów ich zabezpieczenia;

e) przetwarzanie danych osobowych niezgodnie z założonym zakresem i celem ich zbierania;

f) spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nieuprawnione kopiowanie danych osobowych;

g) naruszenie praw osób, których dane są przetwarzane.

5. 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.
6. 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 z przetwarzających Dane osobowe był pisemnie upoważniony do przetwarzania zgodnie z „Upoważnieniem do przetwarzania danych osobowych" – wzór Upoważnienia stanowi **Załącznik nr 2** do niniejszej Polityki.
7. Administrator Danych dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie pracowników i współpracowników i zmianach ról osób oraz zmianach podmiotów przetwarzających.
8. Pracownicy i współpracownicy zobowiązani są 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.

VI. Obszar przetwarzania danych osobowych

1. Obszar, w którym przetwarzane są Dane osobowe: **ul. Łuczanowicka 30 oraz Ujastek 1 w Krakowie** - obszary te obejmują pomieszczenia biurowe Administratora Danych oraz hale produkcyjną.
2. Przetwarzanie Danych osobowych odbywa się również w miejscach wskazanych przez klientów Administratora Danych, w których pracownicy lub współpracownicy wykonują czynności serwisowe lub naprawcze.

VII. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Administrator Danych stosuje ograniczenia dostępu do danych osobowych:

a) prawne (zobowiązania do poufności, zakresy upoważnień, umowy o powierzeniu danych do przetwarzania);

b) fizyczne (strefy dostępu do pomieszczeń, zamykanie pomieszczeń);

c) logiczne (ograniczenia uprawnień do systemów informatycznych i zasobów sieciowych, w których rezydują dane osobowe – loginy i hasła do urządzeń i plików).

2. Zastosowane środki ochrony (techniczne i organizacyjne) są adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych.

3. Stosowane środki ochrony obejmują:

a) 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;

b) zamykanie pomieszczeń tworzących obszar Przetwarzania danych osobowych określony w pkt VII powyżej na czas nieobecności pracowników, w sposób uniemożliwiający dostęp do nich osób trzecich;

c) wykorzystanie zamykanych szafek i sejfów do zabezpieczenia dokumentów;

d) wykorzystanie niszczarki do skutecznego usuwania dokumentów zawierających dane osobowe;

e) ochronę sieci lokalnej przed działaniami inicjowanymi z zewnątrz przy użyciu sieci firewall;

f) wykonywanie kopii awaryjnych danych;

g) ochronę Systemu informatycznego przed złośliwym oprogramowaniem;

h) zabezpieczenie dostępu do urządzeń i Systemu informatycznego przy pomocy haseł dostępu.

VIII. Naruszenia zasad ochrony danych osobowych

1. W przypadku stwierdzenia naruszenia ochrony danych osobowych Administrator Danych dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.

2. W każdej sytuacji, w której zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator Danych zgłasza fakt naruszenia zasad ochrony danych organowi nadzorczemu bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.

3. Wzór zgłoszenia określa **załącznik nr 3** do Polityki. Organem nadzoru jest Prezes Urzędu Ochrony Danych.

4. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator Danych zawiadamia o naruszeniu także osobę, której dane dotyczą.

IX. Powierzenie przetwarzania danych osobowych

1. Administrator Danych może powierzyć przetwarzanie danych osobowych innemu podmiotowi (podmiot przetwarzający) wyłącznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO.
2. Wzór umowy o powierzeniu przetwarzania danych osobowych stanowi **Załącznik nr 5** do niniejszej Polityki.
3. Przed powierzeniem przetwarzania danych osobowych Administrator Danych w miarę możliwości uzyskuje informacje o dotychczasowych praktykach podmiotu przetwarzającego dotyczących zabezpieczenia danych osobowych.

X. Przekazywanie danych do państwa trzeciego

Administrator Danych Osobowych co do zasady nie przekazuje danych osobowych do państwa trzeciego, poza sytuacjami w których następuje to za zgodą osoby, której danych dotyczy takie przekazanie, po spełnieniu obowiązków informacyjnych dotyczących zagrożeń (art. 49 ust. 1 lit. a RODO).

XI. Postanowienia końcowe

1. Za niedopełnienie obowiązków wynikających z niniejszego dokumentu pracownik ponosi odpowiedzialność na podstawie Kodeksu pracy oraz przepisów o ochronie danych osobowych.
2. Integralną część niniejszej Polityki bezpieczeństwa stanowią następujące Załączniki:

   Załącznik nr 1 – Rejestr czynności przetwarzania danych osobowych;

   Załącznik nr 2 – Wzór upoważnienia do przetwarzania danych osobowych;

   Załącznik nr 3 – Wzór oświadczenia i zobowiązania osoby przetwarzającej dane osobowe;

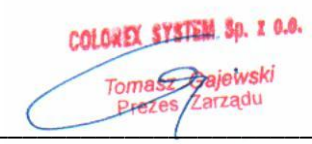
   Załącznik nr 4 – Wzór zgłoszenia naruszenia zasad ochrony danych do organu nadzorczego;

   Załącznik nr 5 – Wzór umowy o powierzeniu przetwarzania danych osobowych.

Niniejszym zatwierdzam Politykę Ochrony Danych Osobowych

oraz przyjmuję ją do stosowania w

COLOREX SYSTEM sp. z o.o.



za Administratora danych osobowych

Tomasz Gajewski- Prezes Zarządu

COLOREX SYSTEM sp. z o.o.