Polityka ochrony danych osobowych w Canna Gold Sp. z o.o.

I. Postanowienia ogólne

Cel Polityki: Niniejsza Polityka Ochrony Danych Osobowych (dalej jako *Polityka*) określa zasady przetwarzania oraz ochrony danych osobowych w spółce **Canna Gold Sp. z o.o.** z siedzibą w Polsce. Jej celem jest zapewnienie zgodności działalności Spółki z obowiązującymi przepisami o ochronie danych osobowych oraz realizacja wymogów bezpieczeństwa i legalności przetwarzania danych. Dokument ten stanowi jedną z wewnętrznych regulacji wdrożonych przez Spółkę w ramach realizacji zasady **rozliczalności** określonej w art. 5 ust. 2 RODO – Administrator wdrażając odpowiednie środki organizacyjne (w tym polityki ochrony danych) jest w stanie wykazać przestrzeganie przepisów RODO. Polityka została opracowana w oparciu o przepisy **RODO** (Rozporządzenia UE 2016/679) – w szczególności z uwzględnieniem art. 24 ust. 2, art. 32 ust. 2 oraz motywu 78 RODO – a także zgodnie z wymogami **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych** obowiązującej w Polsce.

Zakres stosowania: Polityka ma zastosowanie do wszelkich operacji na danych osobowych prowadzonych w Spółce, niezależnie od formy (elektronicznej czy papierowej) i kategorii osób, których dane dotyczą. Obowiązuje ona wszystkich pracowników oraz współpracowników Canna Gold Sp. z o.o., którzy przetwarzają dane osobowe w ramach swoich obowiązków służbowych. Każda osoba mająca dostęp do danych osobowych jest zobowiązana do przestrzegania zasad niniejszej Polityki. Za wdrożenie i utrzymanie Polityki odpowiedzialny jest Zarząd Spółki, który wyznacza osoby nadzorujące obszar ochrony danych osobowych. Nadzór nad przestrzeganiem zasad Polityki sprawuje również – o ile został powołany – **Inspektor Ochrony Danych (IOD)** lub inna wyznaczona osoba ds. Zgodności.

Dostępność Polityki: Dokument ten jest traktowany jako jawny i ogólnodostępny – Spółka udostępnia Politykę wszystkim zainteresowanym stronom (na swojej stronie internetowej), tak aby również osoby, których dane jeszcze nie są przez Spółkę przetwarzane, mogły zapoznać się z zasadami ochrony danych obowiązującymi w Canna Gold.

II. Definicje podstawowych pojęć

Dla lepszego zrozumienia Polityki poniżej przedstawiono definicje kluczowych terminów (zgodne z RODO i polskimi przepisami):

- **Dane osobowe** – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą). Osobą możliwą do zidentyfikowania jest taka, którą można bezpośrednio lub pośrednio rozpoznać, w szczególności na podstawie identyfikatora takiego jak imię, nazwisko, numer identyfikacyjny (PESEL, NIP itp.), dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość tej osoby.
- **Przetwarzanie** – jakakolwiek operacja lub zestaw operacji wykonywanych na danych osobowych, w sposób zautomatyzowany lub nie, takimi jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptacja lub modyfikacja, odczytywanie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowanie lub łączenie, ograniczanie, usunięcie lub zniszczenie (definicja zgodna z art. 4 pkt 2 RODO).
- **Administrator danych** – **Canna Gold Sp. z o.o.**, czyli podmiot decydujący o celach i sposobach przetwarzania danych osobowych. Administrator ponosi odpowiedzialność za zgodność przetwarzania z prawem oraz za realizację zasad ochrony danych. W kontekście niniejszej Polityki terminy *Administrator* i *Spółka* są używane zamiennie.
- **Inspektor Ochrony Danych (IOD)** – osoba wyznaczona przez Administratora do pełnienia funkcji nadzorczych i doradczych w obszarze ochrony danych osobowych, zgodnie z art. 37–39 RODO. Obowiązek wyznaczenia IOD zachodzi w przypadkach określonych w art. 37 RODO (np. przetwarzanie na dużą skalę szczególnych kategorii danych); jeśli w Spółce nie powołano formalnie IOD (bo nie jest to wymagane prawem), Administrator wyznacza innego pracownika lub specjalistę pełniącego rolę koordynatora ds. ochrony danych i realizującego zadania analogiczne do zadań IOD.
- **Podmiot przetwarzający** – każda osoba trzecia lub firma, która przetwarza dane osobowe w imieniu Administratora na podstawie zawartej ze Spółką umowy powierzenia (np. zewnętrzna firma IT, dostawca usług hostingu, biuro księgowe). Podmiot przetwarzający jest zobowiązany do zapewnienia odpowiednich środków ochrony danych i przetwarza dane wyłącznie na udokumentowane polecenie Administratora.

- **RODO – 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 swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych). RODO jest bezpośrednio stosowane we wszystkich krajach UE, w tym w Polsce, od 25 maja 2018 r. i ustanawia jednolite zasady ochrony danych osobowych.
- **Ustawa o ochronie danych osobowych** – polska ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781 t.j.), która uzupełnia i doprecyzowuje krajowy system ochrony danych w związku z RODO (między innymi regulując zasady powoływania IOD w podmiotach publicznych, procedury kontroli i sankcje administracyjne w Polsce).
- **Profilowanie** – dowolna forma zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu tych danych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby, jej sytuacji ekonomicznej, zdrowotnej, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się. W kontekście RODO profilowanie może prowadzić do decyzji wywołujących skutki prawne dla osoby lub w podobny sposób istotnie na nią wpływających (art. 22 RODO).

(Pozostałe terminy użyte w Polityce należy rozumieć zgodnie z definicjami zawartymi w RODO i innych właściwych przepisach. W razie wątpliwości interpretacyjnych, definicje ustawowe mają pierwszeństwo przed zapisami Polityki.)

III. Podstawy prawne przetwarzania danych

Canna Gold Sp. z o.o. działa w oparciu o obowiązujące prawo i przetwarza dane osobowe **zgodnie z przepisami RODO oraz polskimi regulacjami**. W szczególności przyjęto poniższe akty prawne jako podstawę opracowania i wdrożenia niniejszej Polityki:

- **RODO (Rozporządzenie UE 2016/679)** – kompleksowy akt prawny regulujący zasady ochrony danych osobowych w UE, bezpośrednio obowiązujący i nadrzędny wobec krajowych przepisów w zakresie objętym jego regulacją. W art. 24 ust. 2 RODO wprost wskazano, że wdrożenie odpowiednich **polityk ochrony danych** jest jednym ze środków zapewniających zgodność przetwarzania z RODO. Ponadto art. 32 RODO wymaga zastosowania przez administratora i podmiot przetwarzający środków technicznych i organizacyjnych zapewniających odpowiedni poziom bezpieczeństwa danych – niniejsza Polityka

spełnia również ten wymóg poprzez ustanowienie organizacyjnych ram bezpieczeństwa. Motyw 78 RODO zachęca administratorów do wdrażania wewnętrznych **polityk ochrony danych**, uwzględniających zasady privacy by design i privacy by default podczas przetwarzania danych.

- **Ustawa o ochronie danych osobowych z 10 maja 2018 r.** – polska ustawa krajowa, która uzupełnia RODO, m.in. określając organ nadzorczy (Prezes Urzędu Ochrony Danych Osobowych, PUODO), procedury postępowania w sprawach naruszeń ochrony danych, obowiązek wyznaczenia IOD dla niektórych podmiotów oraz odpowiedzialność karną i administracyjne kary za naruszenia. Spółka przestrzega przepisów tej ustawy tam, gdzie mają one zastosowanie (np. w zakresie współpracy z organem nadzorczym, zasad prowadzenia postępowań kontrolnych, notyfikacji wyznaczenia IOD itp.).
- **Inne przepisy sektorowe i wykonawcze:** W razie, gdy szczególne przepisy prawa polskiego lub unijnego nakładają dodatkowe obowiązki w zakresie ochrony danych (np. ustawy branżowe regulujące przetwarzanie danych zdrowotnych, finansowych, pracowniczych; rozporządzenia dotyczące dokumentacji przetwarzania danych w podmiotach publicznych itp.), Spółka uwzględnia wymagania tych regulacji w swojej działalności. Polityka może być uzupełniona wewnętrznymi procedurami dostosowanymi do takich przepisów, jeśli jest to konieczne dla zapewnienia pełnej zgodności z prawem.

Podstawy prawne przetwarzania danych w Spółce: Każda operacja przetwarzania danych osobowych w Canna Gold Sp. z o.o. opiera się na co najmniej jednej z przesłanek legalizujących przetwarzanie, określonych w art. 6 ust. 1 RODO. Oznacza to, że Spółka przetwarza dane **wyłącznie gdy spełniony jest przynajmniej jeden z warunków**: (i) osoba, której dane dotyczą wyraziła na to **dobrowolną zgodę**, (ii) przetwarzanie jest **niezbędne do wykonania umowy** lub do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą, (iii) przetwarzanie jest **niezbędne do wypełnienia obowiązku prawnego** ciążącego na Administratorze (np. wynikającego z przepisów podatkowych, o rachunkowości, prawa pracy), (iv) przetwarzanie jest **niezbędne do celów wynikających z prawnie uzasadnionych interesów** realizowanych przez Administratora lub stronę trzecią – przy czym w takiej sytuacji Spółka każdorazowo ocenia, czy interesy te nie są nadrzędne wobec praw i wolności osoby, której dane dotyczą. W razie, gdyby przetwarzano dane szczególnych kategorii (wrażliwe) określone w art. 9 RODO, Spółka zapewnia istnienie jednej z dodatkowych podstaw wymienionych w art. 9 ust. 2 (np. wyraźna zgoda osoby na przetwarzanie jej danych zdrowotnych w konkretnym celu, przetwarzanie w ramach obowiązków w dziedzinie prawa pracy, ochrony zdrowia, ustalenia roszczeń prawnych itp.). **Canna Gold nie przetwarza danych wrażliwych ani danych dotyczących**

wyroków/naruszeń prawa (art. 10 RODO) w swojej bieżącej działalności, chyba że jest to absolutnie konieczne i zgodne z prawem (np. dane o zdrowiu pracowników do celów BHP lub zaświadczenia o niekaralności wymagane przepisami) – w takich przypadkach Spółka stosuje szczególne środki ochrony i spełnia wszystkie wymagania wynikające z RODO.

IV. Zakres, cele i charakter przetwarzania danych w Spółce

Kategorie danych i osób: W ramach swojej działalności Canna Gold Sp. z o.o. może przetwarzać dane osobowe następujących kategorii osób fizycznych: (1) **pracowników i współpracowników** Spółki (dane kadrowe, identyfikacyjne, kontaktowe, informacje niezbędne do zatrudnienia i rozliczeń itp.), (2) **kontrahentów, klientów lub ich reprezentantów** (dane potrzebne do zawarcia i wykonania umów, obsługi zamówień, świadczenia usług, komunikacji biznesowej), (3) **dostawców i partnerów biznesowych** (dane osób kontaktowych, pełnomocników, konieczne do realizacji umów i płatności), oraz ewentualnie (4) **użytkowników strony internetowej lub osób kontaktujących się ze Spółką** (np. dane w formularzach kontaktowych, adresy e-mail zapytań). Spółka **nie kieruje swoich usług do dzieci** poniżej 16 roku życia i co do zasady nie przetwarza świadomie ich danych osobowych. Gdyby w wyjątkowych sytuacjach doszło do przetwarzania danych dziecka, Spółka zapewni uzyskanie zgody opiekuna prawnego dziecka, o ile jest wymagana przez prawo, zgodnie z art. 8 RODO.

Cele przetwarzania: Canna Gold Sp. z o.o. przetwarza dane osobowe wyłącznie w jasno określonych i zgodnych z prawem celach. Do głównych celów należą przede wszystkim:

- **Realizacja umów i usług** – przetwarzanie danych klientów lub kontrahentów w celu zawarcia umowy, świadczenia zamówionych usług lub dostarczenia towarów, a także obsługi posprzedażowej, rozpatrywania reklamacji itp. (podstawa: niezbędność do wykonania umowy lub działania przedumowne na żądanie osoby).
- **Obowiązki prawne** – przetwarzanie danych w celu wypełnienia obowiązków wynikających z przepisów prawa ciążących na Spółce, np. obowiązków księgowych i podatkowych (wystawianie i przechowywanie faktur z danymi), obowiązków z zakresu prawa pracy i ubezpieczeń społecznych (dane pracowników), obowiązków archiwizacyjnych, udzielania odpowiedzi organom władzy publicznej itp. (podstawa: obowiązek prawny).

- **Zarządzanie przedsiębiorstwem i uzasadnione interesy** – prowadzenie wewnętrznych rejestrów i ewidencji (np. rejestr kontrahentów, rejestr korespondencji), zapewnienie bezpieczeństwa fizycznego obiektów (monitoring wizyjny, jeśli jest stosowany – przy poszanowaniu prywatności), dochodzenie lub obrona przed roszczeniami prawnymi, zapobieganie nadużyciom i oszustwom, wewnętrzna administracja IT (logi systemowe itp.), a także podstawowa komunikacja marketingowa z obecnymi klientami dotycząca własnych produktów/usług (soft marketing, o ile mieści się w ramach prawnie uzasadnionego interesu). W każdym przypadku, gdy Spółka powołuje się na swój **prawnie uzasadniony interes** jako podstawę przetwarzania, dokonuje tzw. **testu równowagi**, aby upewnić się, że interesy lub podstawowe prawa i wolności osób, których dane dotyczą, nie mają charakteru nadrzędnego.

Brak działań marketingowych i profilowania: Spółka **nie przetwarza danych osobowych w celach marketingu bezpośredniego ani w celach profilowania** osób fizycznych. Oznacza to, że Canna Gold Sp. z o.o. nie wysyła niezamówionych informacji handlowych (spam) do osób, których danych nie uzyskała na podstawie ważnej zgody lub innej podstawy prawnej, nie prowadzi newslettera ani kampanii mailingowych skierowanych do osób fizycznych, a także nie buduje profili klientów w celu przewidywania ich preferencji czy automatycznego podejmowania decyzji. Ponadto **Spółka nie sprzedaje ani nie przekazuje danych osobowych osobom trzecim** do ich własnych celów komercyjnych – dane nie są **towarem** i nie podlegają komercyjnej wymianie. Administrator danych **nie udostępnia, nie sprzedaje, nie przekazuje ani w żaden inny sposób nie rozpowszechnia danych osobowych** podmiotom trzecim i nie zamierza tego robić w przyszłości, chyba że: (i) obowiązek takiego udostępnienia wynika z bezwzględnie obowiązującego przepisu prawa, (ii) jest to niezbędne do wykonania zawartej umowy lub świadczenia usługi na rzecz osoby, której dane dotyczą, lub (iii) osoba wyraziła na to wyraźną zgodę. Przykładowo, przekazanie adresu klienta i szczegółów zamówienia partnerowi logistycznemu może być konieczne w celu dostarczenia przesyłki – nie jest to jednak *sprzedaż danych*, lecz działanie w ramach realizacji usługi dla klienta. W razie jakichkolwiek przyszłych zmian w tym zakresie (np. planowanego wprowadzenia marketingu bezpośredniego), Spółka z wyprzedzeniem poinformuje osoby, których dane dotyczą, spełniając obowiązki informacyjne RODO i respektując prawo do sprzeciwu.

Charakter i sposób przetwarzania: Przetwarzanie danych w Spółce odbywa się zarówno w sposób **tradycyjny (papierowy)**, jak i **elektroniczny** – z wykorzystaniem systemów informatycznych. Dane osobowe przechowywane są głównie w zabezpieczonych systemach komputerowych oraz ewentualnie w formie papierowej w siedzibie Spółki. Każdy proces przetwarzania danych jest poprzedzony analizą pod

kątem minimalizacji – zbieramy tylko takie dane, które są niezbędne do osiągnięcia danego celu (szczegółowe zasady minimalizacji opisano w sekcji dot. **Zasad przetwarzania**). Dane przetwarzane są przez upoważnione osoby, zgodnie z nadanymi im rolami i zakresem obowiązków, co zapobiega niekontrolowanemu dostępowi. Spółka wdrożyła odpowiednie zabezpieczenia techniczne i organizacyjne, aby zapewnić poufność, integralność i dostępność danych na każdym etapie przetwarzania (szczegóły w sekcji **Bezpieczeństwo danych**).

V. Podstawowe zasady przetwarzania danych osobowych

Canna Gold Sp. z o.o. przestrzega **podstawowych zasad przetwarzania danych osobowych** wynikających z art. 5 RODO. Zasady te stanowią fundament wszelkich operacji na danych w Spółce i są następujące:

- **Zgodność z prawem, rzetelność i przejrzystość** – wszelkie dane osobowe są przetwarzane legalnie, to znaczy wyłącznie na dopuszczalnych podstawach prawnych, oraz rzetelnie (uczciwie wobec osób, których dane dotyczą). Spółka dba o *przejrzystość* przetwarzania, co oznacza, że informuje osoby o celach i sposobach wykorzystania ich danych w zrozumiały sposób. Każda osoba, której dane dotyczą, ma jasność co do tego, **kto** (Administrator), **w jakim celu** i **jak** przetwarza jej dane – realizowane jest to poprzez odpowiednie klauzule informacyjne przekazywane przy pozyskiwaniu danych (zgodnie z art. 13 lub 14 RODO).
- **Ograniczenie celu** – dane są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i **nie są dalej przetwarzane w sposób niezgodny z tymi celami**. Spółka ściśle definiuje cele zbierania danych (por. sekcja powyżej) i **nie wykorzystuje danych w nowych celach**, które byłyby niezgodne z pierwotnym celem ich zebrania. Ewentualne przetwarzanie danych w celach archiwalnych, naukowych, statystycznych itp. odbywa się z zachowaniem wymogów art. 89 ust. 1 RODO, tak by nie było sprzeczne z pierwotnymi celami.
- **Minimalizacja danych** – Spółka stosuje zasadę *„tyle danych, ile to konieczne”*. Przetwarzane dane osobowe są **adekwatne, stosowne oraz ograniczone** do tego, co niezbędne w relacji do celów, w jakich są przetwarzane. W praktyce oznacza to, że przed zebraniem danych analizujemy, jakie informacje są rzeczywiście potrzebne (np. do zawarcia umowy wymagamy danych niezbędnych do identyfikacji stron i realizacji świadczenia, ale nie zbieramy nadmiarowych informacji). Unikamy gromadzenia na zapas danych, które mogą nigdy nie być wykorzystywane. Także okres przechowywania danych jest

dostosowany do niezbędnego minimum – po osiągnięciu celu dane są usuwane lub anonimizowane (zasada ograniczenia przechowywania, patrz niżej).

- **Prawidłowość (dokładność) danych** – Canna Gold dba o to, by dane osobowe pozostawały **prawidłowe i w razie potrzeby aktualne**. Podejmujemy rozsądne działania, aby dane nieprawidłowe (błędne lub nieaktualne) zostały niezwłocznie sprostowane lub zaktualizowane. Osoby, których dane dotyczą, mają prawo do sprostowania swoich danych, a Spółka zapewnia łatwe mechanizmy zgłaszania zmian (np. aktualizacja danych kontaktowych klienta na jego żądanie, korekta danych pracownika). Regularnie weryfikujemy posiadane bazy danych pod kątem ich aktualności – np. w odniesieniu do pracowników aktualizujemy dane adresowe, w odniesieniu do kontrahentów monitorujemy ważność umów i związane z tym dane kontaktowe.
- **Ograniczenie przechowywania** – dane osobowe są przechowywane **w formie umożliwiającej identyfikację osoby, której dane dotyczą, nie dłużej niż to konieczne** do realizacji celów, w których dane te są przetwarzane. Innymi słowy, Spółka stosuje ustalone okresy retencji danych. Po upływie okresu niezbędnego dla danego celu, dane są trwale usuwane lub poddawane anonimizacji (chyba że dalsze przechowywanie jest wymagane przepisami prawa – np. przechowywanie dokumentacji księgowej przez ustawowy okres 5 lat, przechowywanie akt osobowych pracownika przez wymagany przepisami czas itp.). Harmonogramy przechowywania danych zostały określone w odrębnych procedurach wewnętrznych (polityka retencji) i są przestrzegane przez pracowników. Jeśli dane osobowe są potrzebne dłużej wyłącznie do celów archiwalnych, badań naukowych, historycznych lub statystycznych – Spółka zapewnia odpowiednie środki (np. pseudonimizację, ograniczenie dostępu) w celu ochrony praw osób, zgodnie z art. 89 ust.1 RODO.
- **Integralność i poufność** – Spółka przetwarza dane w sposób zapewniający odpowiednie **bezpieczeństwo** danych osobowych. Obejmuje to ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem, jak również przed przypadkową utratą, zniszczeniem lub uszkodzeniem danych. Wdrożono adekwatne środki techniczne i organizacyjne, aby zagwarantować **poufność** (dostęp do danych mają wyłącznie upoważnione osoby, zobowiązane do tajemnicy), **integralność** (dane są chronione przed nieautoryzowaną modyfikacją, stosuje się mechanizmy kontroli integralności, kopie zapasowe) oraz **dostępność** danych (dane są zabezpieczone przed utratą, a w razie awarii systemów możliwe jest ich przywrócenie z kopii zapasowych w odpowiednim czasie). Szczegółowe środki bezpieczeństwa opisano w rozdziale **Bezpieczeństwo danych** niniejszej Polityki.

- **Rozliczalność** – Administrator (Spółka) ponosi odpowiedzialność za przestrzeganie powyższych zasad i **musi być w stanie wykazać** ich przestrzeganie. Zasada rozliczalności oznacza, że Canna Gold dokumentuje procesy przetwarzania danych (prowadzi wymagane rejestry, np. Rejestr Czynności Przetwarzania), wydaje upoważnienia do przetwarzania dla personelu, posiada niniejszą Politykę oraz wdrożone procedury postępowania, a w razie kontroli organu nadzorczego lub dochodzenia praw osób – jest w stanie przedstawić dowody na zgodność swoich działań z RODO. W praktyce realizujemy rozliczalność m.in. poprzez regularne **audyty wewnętrzne** w zakresie ochrony danych, sporządzanie raportów z tych audytów oraz korygowanie ewentualnych stwierdzonych niezgodności.

Uwzględnienie ochrony danych w projektowaniu: Spółka zobowiązuje się stosować zasadę **privacy by design** (ochrona danych w fazie projektowania) oraz **privacy by default** (domyślna ochrona danych). Oznacza to, że już na etapie planowania nowych procesów biznesowych, usług, systemów informatycznych czy rozwiązań organizacyjnych, uwzględniamy kwestie ochrony danych osobowych – tak aby zapobiegać naruszeniom prywatności jeszcze zanim one wystąpią. Domyślna ochrona danych oznacza zaś, że standardowe ustawienia i procedury gwarantują najwyższy poziom prywatności (np. domyślnie zbieramy tylko te dane, które są potrzebne, a pola opcjonalne są wyraźnie oznaczone; systemy IT domyślnie nie udostępniają publicznie żadnych zebranych danych, chyba że użytkownik sam to wybierze itd.). Wszelkie nowe przedsięwzięcia w Spółce przechodzą **analizę ryzyka dla ochrony danych** – oceniamy, jakie zagrożenia dla prywatności mogą wiązać się z danym procesem i jak je zminimalizować. Gdy planowane operacje na danych mogą powodować wysokie ryzyko naruszenia praw lub wolności osób, Spółka przeprowadza formalną **Oceny Skutków dla Ochrony Danych (DPIA)** zgodnie z art. 35 RODO, a następnie wdraża zalecenia wynikające z tej oceny. Polityka wymaga okresowego przeglądu i aktualizacji przeprowadzonych ocen ryzyka oraz DPIA – co najmniej przy każdej istotnej zmianie okoliczności przetwarzania (np. wprowadzeniu nowej technologii, zmiany zakresu danych).

VI. Prawa osób, których dane dotyczą

Spółka respektuje wszystkie prawa przysługujące osobom fizycznym, których dane osobowe są przetwarzane. RODO gwarantuje osobom szereg praw i mechanizmów kontroli nad własnymi danymi. W celu zapewnienia przejrzystości poniżej przedstawiamy przysługujące prawa oraz sposób ich realizacji w Canna Gold Sp. z o.o.:

- **Prawo dostępu do danych (art. 15 RODO)** – każda osoba ma prawo uzyskać od Spółki potwierdzenie, czy przetwarzamy jej dane osobowe, a jeżeli ma to miejsce – prawo otrzymać kopię danych oraz wszelkie informacje o przetwarzaniu, m.in. o celach, kategoriach danych, odbiorcach, planowanym okresie przechowywania, źródłach danych itp. Na żądanie osoby udzielamy jej wyczerpujących informacji oraz udostępniamy kopie posiadanych danych w formie papierowej lub elektronicznej.
- **Prawo do sprostowania danych (art. 16 RODO)** – na wniosek osoby niezwłocznie korygujemy dotyczące jej dane osobowe, które są nieprawidłowe, oraz uzupełniamy dane niekompletne (w razie potrzeby złożenia dodatkowego oświadczenia przez osobę). Dbamy, aby dane wykorzystywane przez Spółkę były aktualne i dokładne – każdy błąd zgłoszony przez osobę jest bezzwłocznie poprawiany.
- **Prawo do usunięcia danych, tzw. „prawo do bycia zapomnianym" (art. 17 RODO)** – osoba ma prawo żądać usunięcia swoich danych, a Spółka jest zobowiązana je usunąć, jeśli zachodzi jedna z przesłanek przewidzianych w art. 17 RODO, np.: dane nie są już potrzebne do celów, dla których zostały zebrane, osoba wycofała zgodę (i brak innej podstawy prawnej), osoba wniosła sprzeciw wobec przetwarzania i brak nadrzędnych prawnie uzasadnionych podstaw przetwarzania, dane były przetwarzane niezgodnie z prawem, lub muszą zostać usunięte w celu wywiązania się z obowiązku prawnego. **UWAGA:** Prawo do usunięcia nie ma charakteru bezwzględnego – w pewnych sytuacjach nie możemy usunąć danych mimo żądania osoby (np. gdy przetwarzanie jest konieczne do wywiązania się z obowiązku prawnego lub do ustalenia, dochodzenia lub obrony roszczeń – art. 17 ust. 3 RODO). W odpowiedzi na żądanie usunięcia analizujemy, czy nie zachodzą te wyjątki. Jeżeli dane zostały upublicznione (czego Spółka co do zasady nie czyni), podejmujemy rozsądne działania, by poinformować innych administratorów przetwarzających te dane o konieczności usunięcia wszelkich linków, kopii itp.
- **Prawo do ograniczenia przetwarzania (art. 18 RODO)** – w określonych sytuacjach (np. gdy osoba kwestionuje prawidłowość danych, gdy przetwarzanie jest niezgodne z prawem, ale osoba sprzeciwia się ich usunięciu, gdy Spółce dane nie są już potrzebne, ale osobie są potrzebne do ustalenia roszczeń, lub gdy osoba wniosła sprzeciw – do czasu rozpatrzenia sprzeciwu) osoba może żądać, by **ograniczyć przetwarzanie jej danych wyłącznie do przechowywania** lub wykonania uzgodnionych z nią działań. W razie realizacji takiego uprawnienia, Spółka nie będzie dokonywać na danych żadnych operacji poza przechowaniem (ewentualnie zabezpieczeniem) – chyba że za zgodą osoby lub w celu ustalenia, dochodzenia, obrony roszczeń bądź ochrony praw innej

osoby fizycznej lub z uwagi na ważne względy interesu publicznego. O uchyleniu ograniczenia (jeśli nastąpi) poinformujemy osobę z wyprzedzeniem.

- **Prawo do przenoszenia danych (art. 20 RODO)** – w przypadku, gdy dane są przetwarzane na podstawie zgody osoby lub na podstawie umowy z nią zawartej oraz w sposób zautomatyzowany – osoba ma prawo otrzymać od nas swoje dane osobowe, które nam dostarczyła, w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego (np. CSV, XML). Może też zażądać, byśmy **przekazali te dane bezpośrednio innemu administratorowi**, o ile jest to technicznie możliwe. Przy realizacji prawa do przenoszenia dbamy, aby nie wpływało ono negatywnie na prawa i wolności innych osób (np. anonimizujemy dane innych osób, które mogłyby znajdować się w zbiorze przekazywanych danych).
- **Prawo do sprzeciwu wobec przetwarzania (art. 21 RODO)** – osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść **sprzeciw** z przyczyn związanych z jej szczególną sytuacją wobec przetwarzania jej danych opartego na przesłance prawnie uzasadnionych interesów Administratora (art. 6 ust.1 lit. f) lub na zadaniu realizowanym w interesie publicznym (lit. e). W takim przypadku po otrzymaniu sprzeciwu **zaprzestaniemy przetwarzania tych danych**, chyba że wykażemy istnienie ważnych, prawnie uzasadnionych podstaw do przetwarzania, które są nadrzędne wobec interesów, praw i wolności osoby lub podstaw do ustalenia, dochodzenia lub obrony roszczeń. **Jeżeli jednak sprzeciw dotyczy przetwarzania danych na potrzeby marketingu bezpośredniego, uwzględniamy go zawsze** – w razie sprzeciwu wobec marketingu (w tym ewentualnego profilowania marketingowego) Spółka niezwłocznie zaprzestanie takiego przetwarzania. Ponieważ obecnie Spółka nie prowadzi marketingu bezpośredniego, prawo sprzeciwu ma zastosowanie głównie do ewentualnego przetwarzania danych na podstawie uzasadnionego interesu – już na etapie zbierania danych informujemy osoby o istnieniu prawa sprzeciwu oraz o sposobie jego zgłoszenia.
- **Prawo niepodlegania zautomatyzowanemu podejmowaniu decyzji (art. 22 RODO)** – Spółka nie podejmuje wobec osób decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu, które wywoływałyby wobec tych osób skutki prawne lub w podobny sposób istotnie na nie wpływały. Gdyby jednak takie operacje były w przyszłości realizowane (np. profilowanie klientów w celu automatycznego przyznania określonych warunków usługi), osobie przysługiwałoby prawo do **niepodlegania takiej decyzji** oraz do uzyskania **interwencji ludzkiej** po stronie Administratora, wyrażenia własnego stanowiska i zakwestionowania decyzji. Spółka zapewni realizację tych uprawnień, jeśli zastosowałaby kiedykolwiek w pełni zautomatyzowane mechanizmy decyzyjne.

- **Prawo do wycofania zgody** – w sytuacji, gdy podstawą przetwarzania danych osobowych jest zgoda osoby (art. 6 ust.1 lit. a RODO lub art. 9 ust.2 lit. a dla danych wrażliwych), osoba ta ma prawo w dowolnym momencie **cofnąć udzieloną zgodę**. Wycofanie zgody nie wpływa na legalność przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem, jednak oznacza, że nie będziemy dalej przetwarzać danych w celu objętym wycofaną zgodą. O możliwości wycofania zgody informujemy zawsze w momencie jej zbierania. Spółka ułatwia wycofanie zgody – może to nastąpić np. poprzez wysłanie e-maila na wskazany kontakt lub kliknięcie stosownego linku (jeśli zgoda była wyrażona elektronicznie).

Realizacja praw przez osobę: Każda osoba, której dane przetwarza Canna Gold, może zgłosić się do Spółki z żądaniem realizacji swoich praw. W tym celu udostępniamy wygodne kanały komunikacji – w szczególności można kontaktować się pisemnie (listownie na adres siedziby) lub mailowo (na oficjalny adres kontaktowy Spółki lub adres Inspektora Ochrony Danych, jeśli został powołany). Wniosek można złożyć w dowolnej formie, byle zawierał informacje pozwalające nam zweryfikować tożsamość wnioskodawcy i zrozumieć zakres żądania. Odpowiadamy bez zbędnej zwłoki – co do zasady **w ciągu miesiąca** od otrzymania żądania. Termin ten może zostać przedłużony maksymalnie o kolejne dwa miesiące w razie potrzeby (z uwagi na skomplikowany charakter żądania lub liczbę żądań), ale wówczas w terminie miesiąca poinformujemy osobę o przyczynie przedłużenia. Realizacja praw jest co do zasady **bezpłatna**. Jeżeli jednak żądania osoby byłyby ewidentnie nieuzasadnione lub nadmierne (np. z powodu ich ustawicznego powtarzania się), Spółka może – zgodnie z art. 12 ust.5 RODO – pobrać rozsądną opłatę uwzględniającą koszty administracyjne realizacji żądania albo odmówić podjęcia działań w związku z żądaniem. Każde zgłoszone żądanie praw osoby rejestrujemy i dokumentujemy sposób jego załatwienia, aby móc wykazać rozliczalność.

Zawiadamianie odbiorców o sprostowaniu/usunięciu/ograniczeniu: Jeśli Spółka sprostuje, usunie lub ograniczy przetwarzanie czyichś danych na żądanie tej osoby, a dane te były uprzednio **udostępnione odbiorcom** (np. przekazane do naszego biura rachunkowego lub do firmy kurierskiej), w miarę możliwości poinformujemy tych odbiorców o dokonaniu sprostowania, usunięcia lub ograniczenia przetwarzania, zgodnie z art. 19 RODO. Nie musimy tego robić tylko, jeśli okazałoby się to niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku (o czym poinformujemy osobę). Na żądanie osoby udzielimy jej informacji o tych odbiorcach.

Prawo wniesienia skargi do organu nadzorczego: Niezależnie od powyższych uprawnień, każda osoba ma prawo **złożyć skargę** do właściwego organu nadzorczego

ds. ochrony danych osobowych. W Polsce organem tym jest **Prezes Urzędu Ochrony Danych Osobowych (UODO)**. Skargę można wnieść, jeżeli zdaniem osoby przetwarzanie danych narusza przepisy RODO lub inne przepisy o ochronie danych. Aktualne dane kontaktowe Urzędu (adres, infolinia) dostępne są na stronie . Spółka informuje osoby o prawie do skargi już w momencie zbierania danych (w klauzulach informacyjnych). Mamy nadzieję, że nie dojdzie do sytuacji, w której będziemy przetwarzać dane niezgodnie z prawem, jednak jeżeli **prawa osób nie są realizowane lub przetwarzanie narusza RODO – osoba może złożyć skargę do Prezesa UODO**, a w razie powstania szkody ma również prawo wystąpić z roszczeniem o odszkodowanie przeciwko Administratorowi. Zachęcamy jednak, aby w pierwszej kolejności zgłaszać wszelkie zastrzeżenia bezpośrednio do nas – niezwłocznie je wyjaśnimy i postaramy się sprostać oczekiwaniom, mając na uwadze najwyższe standardy ochrony danych.

VII. Udostępnianie danych podmiotom zewnętrznym

Zasada ograniczonego udostępniania: Spółka co do zasady **nie udostępnia danych osobowych innym podmiotom**, chyba że istnieje ku temu wyraźna podstawa prawna lub operacyjna konieczność. Jak wspomniano wyżej, Canna Gold Sp. z o.o. nie prowadzi komercyjnej sprzedaży baz danych ani nie przekazuje danych osobowych innym administratorom dla ich własnych celów marketingowych. Możliwe sytuacje udostępnienia danych na zewnątrz obejmują przede wszystkim:

- **Udostępnienie na podstawie prawa** – gdy obowiązek przekazania danych wynika z przepisów prawa, Spółka wykonuje takie obowiązki. Dotyczy to w szczególności żądań uprawnionych organów państwowych (np. sądów, prokuratury, Policji, organów podatkowych, ZUS) – w granicach określonych przez prawo przekazujemy tym organom żądane informacje. Przed ujawnieniem danych zawsze weryfikujemy podstawę prawną żądania i tożsamość wnioskującego organu.
- **Udostępnienie w oparciu o zgodę osoby** – jeżeli osoba, której dane dotyczą, wyraźnie zgodzi się na udostępnienie jej danych wskazanemu podmiotowi (np. partnerowi biznesowemu Spółki), wówczas takie udostępnienie realizujemy w zakresie i celu wskazanym w zgodzie. Zgoda jest uprzednio pozyskiwana od osoby w formie pozwalającej wykazanie jej faktu (np. pisemnie lub elektronicznie).
- **Udostępnienie niezbędne do ochrony praw Spółki** – w razie, gdyby zaszła potrzeba dochodzenia roszczeń lub obrony przed roszczeniami, Spółka może udostępnić niezbędne dane (np. pełnomocnikom prawnym, firmom

windykacyjnym, biegłym itp.). Takie przypadki traktowane są indywidualnie, z dbałością o zachowanie tajemnicy biznesowej i praw osób.

- **Powierzenie przetwarzania danych podmiotom przetwarzającym** – omówione szerzej poniżej, dotyczy sytuacji, gdy zatrudniamy podwykonawców do usług wymagających dostępu do danych (np. firma IT serwisująca systemy, zewnętrzna księgowość). W takich przypadkach formalnie nie jest to „udostępnienie" w rozumieniu RODO, lecz **powierzenie** – czyli działanie w naszym imieniu i na nasze zlecenie.

Powierzanie przetwarzania danych (podmiotom przetwarzającym): Canna Gold Sp. z o.o., prowadząc działalność, korzysta z usług różnych **dostawców i podwykonawców**, którzy mogą przetwarzać dane osobowe w naszym imieniu. Do typowych kategorii takich **podmiotów przetwarzających** należą m.in.: firmy informatyczne (dostarczające oprogramowanie, hosting danych, serwis sprzętu), biura rachunkowe lub kadrowe obsługujące naszą księgowość i sprawy płacowe, firmy kurierskie dostarczające przesyłki, kancelarie prawne świadczące obsługę prawną, zewnętrzni konsultanci i doradcy, firmy archiwizacyjne, agencje rekrutacyjne (w przypadku procesów rekrutacji), itp. W każdej sytuacji powierzenia danych obowiązują następujące zasady:

- **Umowa powierzenia** – z każdym podmiotem przetwarzającym zawieramy pisemną (również w formie elektronicznej) **umowę powierzenia przetwarzania danych**, zgodnie z art. 28 RODO. Umowa taka precyzuje m.in. zakres i cel przetwarzania danych przez podmiot przetwarzający, rodzaj powierzanych danych, obowiązki i uprawnienia zarówno Administratora, jak i procesora, wymagania co do poufności, bezpieczeństwa informacji, zasad postępowania z danymi po zakończeniu współpracy itp.
- **Wybór zaufanych partnerów** – przed powierzeniem danych weryfikujemy każdego dostawcę pod kątem zdolności do spełnienia wymogów bezpieczeństwa. Wybieramy tylko takich partnerów, którzy dają **wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych** przetwarzania, aby spełnić wymagania RODO i chronić prawa osób, których dane dotyczą. Spółka uzyskuje zapewnienia o stosowanych środkach bezpieczeństwa (np. certyfikacje, raporty z audytów, referencje) i — jeśli to niezbędne — przeprowadza własne **audyty** lub żąda testów zabezpieczeń u kluczowych dostawców.
- **Instrukcje i kontrola** – podmiot przetwarzający działa wyłącznie na udokumentowane polecenie Spółki jako Administratora. W praktyce oznacza to, że dostawca usług może wykorzystywać powierzone dane tylko do celów ściśle określonych przez nas i nie może nimi dysponować we własnym zakresie.

Monitorujemy wykonywanie zadań przez podmioty przetwarzające; w umowach zastrzegamy sobie prawo do kontroli ich działań (np. poprzez audyt lub żądanie informacji). Podmiot przetwarzający jest zobowiązany **zgłaszać nam wszelkie incydenty naruszenia danych** niezwłocznie po ich stwierdzeniu oraz współpracować w zakresie realizacji praw osób, odpowiadania na zapytania organów, zapewniania zgodności z RODO.

- **Poufność i personel** – zapewniamy, by osoby zatrudnione u podmiotów przetwarzających, które będą miały dostęp do danych, były zobowiązane do zachowania poufności (np. poprzez podpisanie odpowiednich klauzul) lub podlegały ustawowemu obowiązkowi zachowania tajemnicy zawodowej.
- **Podpowierzenie** – podmiotom przetwarzającym co do zasady **nie wolno angażować dalszych podprzetwarzających** bez naszej uprzedniej zgody. Jeżeli taka zgoda zostanie udzielona (ogólna lub szczególna), podmiot przetwarzający musi zapewnić, że każdy dalszy podwykonawca spełnia te same rygorystyczne standardy ochrony danych jak on sam.

Wykaz głównych podmiotów przetwarzających, którym Spółka powierza dane (wraz z zakresem powierzonych danych i celem) jest prowadzony jako część Rejestru Czynności Przetwarzania lub odrębny **Rejestr kategorii czynności przetwarzania**. Dokumentacja ta jest dostępna na żądanie organu nadzorczego.

Udostępnianie danych odbiorcom innym niż procesorzy: W niektórych przypadkach Spółka może udostępnić dane również innym odbiorcom, którzy stają się niezależnymi administratorami danych – dotyczy to np. przekazania danych do:

- **Organów publicznych** – jak wspomniano, gdy prawo tego wymaga (np. zgłoszenie danych pracowników do ZUS, przekazanie danych do urzędu skarbowego, odpowiedź na wiążące zapytanie Policji w toczącym się postępowaniu itp.).
- **Partnerów biznesowych** – jeśli dana operacja wymaga współpracy z inną firmą, np. realizujemy wspólnie jakiś projekt dla klienta i potrzebne jest przekazanie danych kontaktowych klienta lokalnemu partnerowi – odbywa się to tylko za zgodą osoby lub w oparciu o inną podstawę prawną (np. uzasadniony interes, jeżeli partner jest podwykonawcą klienta). W takich sytuacjach drugi podmiot staje się odrębnym administratorem danych, odpowiadającym już samodzielnie za zgodność przetwarzania po swojej stronie.

We wszystkich powyższych sytuacjach udostępnienia danych poza strukturę Spółki kierujemy się zasadą **minimalizacji** – przekazujemy tylko te informacje, które są niezbędne danemu odbiorcy do określonego celu (np. w odpowiedzi na zapytanie

organu publicznego ujawniamy tylko zakres danych objęty żądaniem i upoważnieniem prawnym). Każde przekazanie danych dokumentujemy (prowadząc ewidencję udostępnień, jeżeli jest wymagana).

Transfery danych do państw trzecich (poza EOG): Spółka **co do zasady nie przekazuje danych osobowych poza obszar Europejskiego Obszaru Gospodarczego (EOG)**. Przechowywanie i przetwarzanie danych odbywa się na terenie państw EOG, gdzie obowiązują jednolite standardy RODO. Jeżeli w wyjątkowych przypadkach doszłoby do transferu danych do państwa trzeciego (np. korzystamy z usług dostawcy chmurowego mającego serwery poza EOG lub zlecamy zadanie podmiotowi spoza EOG), Spółka zapewni legalność takiego przekazania. Będzie to możliwe tylko wtedy, gdy dany kraj został uznany decyzją Komisji Europejskiej za zapewniający **odpowiedni poziom ochrony** albo – w braku takiej decyzji – gdy zastosujemy **stosowne zabezpieczenia** opisane w RODO, np. standardowe klauzule ochrony danych przyjęte przez Komisję (tzw. SCC), wiążące reguły korporacyjne (BCR) u odbiorcy lub wyjątkowe zgody organu nadzorczego. Osoby, których dane dotyczą, zostaną poinformowane o zamiarze przekazania danych poza EOG na etapie zbierania danych (obowiązek informacyjny z art. 13/14 RODO) wraz z informacją, jakie zabezpieczenie zastosowano. Spółka wymaga też, by odbiorcy w państwach trzecich zobowiązali się umownie do przestrzegania standardów bezpieczeństwa i prywatności odpowiadających wymogom RODO.

VIII. Bezpieczeństwo danych osobowych

Polityka bezpieczeństwa: Canna Gold Sp. z o.o. wdrożyła kompleksowe środki techniczne i organizacyjne w celu zapewnienia ochrony przetwarzanych danych osobowych przed zagrożeniami. Środki te zostały dobrane z uwzględnieniem stanu wiedzy technicznej, kosztów wdrożenia oraz charakteru, zakresu, kontekstu i celów przetwarzania, a także ryzyka naruszenia praw lub wolności osób fizycznych (o różnym prawdopodobieństwie wystąpienia i wadze potencjalnego skutku). Regularnie dokonujemy oceny adekwatności zastosowanych zabezpieczeń i w razie potrzeby je aktualizujemy. Priorytetem jest zapewnienie **poufności, integralności, dostępności** oraz **rozliczalności** danych osobowych i operacji na nich.

Środki organizacyjne:

- Spółka ustanowiła wewnętrzne procedury i instrukcje regulujące bezpieczne przetwarzanie danych (np. procedurę zarządzania hasłami, procedurę reagowania na incydenty, instrukcję obsługi systemów informatycznych, politykę czystego biurka i ekranów itp.).

- Dostęp do danych osobowych został ograniczony wyłącznie do osób, dla których jest to niezbędne z racji pełnionych obowiązków (**zasada need-to-know**). Struktura organizacyjna jest tak zaprojektowana, by jasno określać, kto i w jakim zakresie ma dostęp do poszczególnych kategorii danych. Pracownicy mają przydzielane indywidualne *upoważnienia do przetwarzania danych osobowych* wydawane przez Zarząd. W rejestrze upoważnień odnotowujemy wszystkie osoby dopuszczone do danych oraz zakres ich uprawnień.
- Każda osoba przetwarzająca dane (pracownik etatowy, zleceniobiorca, stażysta itp.) **podpisuje oświadczenie o zachowaniu poufności** danych osobowych oraz informacji chronionych, do których ma dostęp. Obowiązek zachowania tajemnicy trwa także po zakończeniu współpracy z Spółką.
- Prowadzimy **szkolenia pracowników** w zakresie ochrony danych – zarówno wstępne (przy rozpoczynaniu pracy), jak i okresowe. Celem szkoleń jest zapoznanie personelu z przepisami RODO, niniejszą Polityką oraz dobrymi praktykami bezpieczeństwa. Spółka podnosi świadomość personelu, aby każdy rozumiał wagę ochrony danych i potrafił właściwie reagować na potencjalne incydenty.
- Wprowadzono kontrolę fizycznego dostępu do pomieszczeń, w których przetwarzane są dane osobowe – biuro Spółki jest zabezpieczone zamkami, systemem alarmowym, kontrolą dostępu i monitoringiem (jeśli stosowany; monitoring prowadzony jest zgodnie z wymogami prawa pracy i przepisami o monitoringu wizyjnym, a osoby znajdujące się w obszarze monitorowanym są odpowiednio informowane). Dostęp do pomieszczeń z dokumentami mają tylko upoważnione osoby; dokumentacja papierowa z danymi jest przechowywana w zamykanych szafach.
- Zastosowano procedury nadawania i odbierania dostępów do systemów informatycznych zawierających dane – każda osoba ma unikalny identyfikator użytkownika i hasło, które podlegają zasadom złożoności i regularnej zmiany. Uprawnienia są na bieżąco aktualizowane (np. odebranie dostępu po zakończeniu współpracy z pracownikiem, zmiana uprawnień przy zmianie roli).

Środki techniczne:

- Dane osobowe w systemach elektronicznych są zabezpieczone przed nieautoryzowanym dostępem za pomocą mechanizmów uwierzytelniania (silne hasła, w miarę potrzeby uwierzytelnianie dwuskładnikowe) oraz autoryzacji (nadawanie minimalnych niezbędnych uprawnień). Systemy informatyczne są chronione aktualnym oprogramowaniem **antywirusowym i antymalware**, a także zaporami sieciowymi (**firewall**).

- Regularnie wykonujemy **kopie zapasowe (backup)** danych przechowywanych elektronicznie. Kopie te są przechowywane w bezpiecznej lokalizacji, odseparowane od systemów operacyjnych i okresowo testujemy możliwość odtworzenia danych z backupu. Chroni to przed utratą danych w razie awarii, ataku ransomware lub innego zdarzenia losowego.
- Stosujemy szyfrowanie danych tam, gdzie jest to uzasadnione ryzykiem – np. przenośne nośniki z danymi (dyski, pendrive) są zaszyfrowane, laptopy służbowe mają zaszyfrowane dyski, a transmisja wrażliwych informacji przez internet odbywa się z użyciem protokołów szyfrowanych (HTTPS, SSL/TLS, VPN). Wewnętrzne bazy danych mogą wykorzystywać szyfrowanie na poziomie bazy lub tabel z najwrażliwszymi danymi.
- Wprowadziliśmy mechanizmy kontroli integralności danych – systemy odnotowują zmiany dokonywane na danych (logi operacji zawierające m.in. identyfikator użytkownika, znacznik czasu oraz rodzaj operacji). Dzięki temu możliwe jest prześledzenie, kto i kiedy modyfikował lub usuwał dane (zapewnienie rozliczalności i możliwości audytu).
- Dokumenty papierowe zawierające dane osobowe są przetwarzane w kontrolowanych warunkach – niszczarki o odpowiedniej klasie bezpieczeństwa są dostępne i używane do fizycznego niszczenia dokumentów, które nie są już potrzebne. Niepotrzebne wydruki zawierające dane są niszczone niezwłocznie. W trakcie pracy dokumenty nie są pozostawiane bez nadzoru na biurkach.
- Spółka monitoruje stan bezpieczeństwa systemów – logi zdarzeń bezpieczeństwa są przeglądane, krytyczne systemy są objęte monitoringiem w trybie ciągłym (np. alerty w razie próby nieautoryzowanego dostępu). Mamy wdrożony system zarządzania aktualizacjami oprogramowania – na bieżąco instalujemy poprawki bezpieczeństwa i aktualizacje systemów operacyjnych oraz aplikacji używanych do przetwarzania danych. Dzięki temu ograniczamy podatność systemów na nowe zagrożenia.
- Okresowo przeprowadzane są **testy bezpieczeństwa** i analizy podatności naszych systemów (samodzielnie lub we współpracy z zewnętrznymi specjalistami). Wyniki testów służą do doskonalenia zabezpieczeń. Prowadzimy również **analizy ryzyka** – identyfikujemy nowe potencjalne zagrożenia (np. pojawiające się metody ataków) i wdrażamy odpowiednie środki zaradcze.

Polityka haseł i bezpieczeństwo stacji roboczych: Każdy użytkownik systemu informatycznego ma unikalne konto zabezpieczone hasłem. Obowiązują zasady tworzenia haseł (minimalna długość, wymóg użycia cyfr i znaków specjalnych, zakaz używania łatwych fraz itp.) oraz ich okresowej zmiany. Stacje robocze są zabezpieczone hasłem lub innym mechanizmem uwierzytelniania przy wznowieniu pracy (wygaszacz

ekranu z hasłem). Użytkownicy są zobowiązani chronić swoje dane logowania i nie udostępniać ich osobom nieuprawnionym. Wszelkie naruszenia tej zasady są traktowane poważnie i mogą skutkować konsekwencjami służbowymi.

Świadomość zagrożeń: Elementem kultury bezpieczeństwa w Spółce jest bieżące informowanie personelu o potencjalnych zagrożeniach (np. atakach phishingowych) i uczulanie na ostrożność. Każdy pracownik wie, że nie wolno otwierać podejrzanych załączników e-mail od nieznanych nadawców, instalować nieautoryzowanego oprogramowania na służbowym komputerze czy podłączać niezweryfikowanych nośników USB. Takie dobre praktyki są regularnie przypominane na szkoleniach i wewnętrznych biuletynach informacyjnych.

Dostosowanie do ryzyka: Poziom zastosowanych zabezpieczeń jest odpowiedni do zidentyfikowanego ryzyka. Dla danych mniej wrażliwych (np. ogólne dane kontaktowe) ryzyko naruszenia prywatności jest mniejsze, jednak nadal chronimy je przed wyciekiem. Dla danych bardziej wrażliwych (np. danych zdrowotnych pracownika, jeśli takie posiadamy – np. zwolnienia lekarskie, orzeczenia lekarskie) stosujemy dodatkowe ograniczenia dostępu i zabezpieczenia. Regularnie weryfikujemy, czy przyjęte środki nadal są skuteczne – jeśli ryzyko wzrasta (np. pojawia się nowy wektor ataku), odpowiednio wzmacniamy zabezpieczenia.

Ogólny opis zabezpieczeń: Podsumowując, Spółka dokłada wszelkich starań, by środki techniczne i organizacyjne ochrony danych były na bieżąco **aktualizowane i dostosowywane** do zmieniających się warunków. Zabezpieczenia mają zapewnić, że dane **nie dostaną się w niepowołane ręce**, nie zostaną **zmienione lub utracone** w sposób nieautoryzowany, a jednocześnie pozostaną **dostępne** dla uprawnionych użytkowników zawsze, gdy będą potrzebne do realizacji celów przetwarzania. Spółka posiada **plan ciągłości działania** na wypadek poważnej awarii lub incydentu – obejmuje on procedury odtworzenia danych z kopii, awaryjne procedury komunikacji oraz działania minimalizujące skutki naruszeń.

IX. Postępowanie w przypadku naruszenia ochrony danych

Mimo wszelkich wdrożonych zabezpieczeń, istnieje możliwość wystąpienia **incydentu naruszenia ochrony danych osobowych**. Przez naruszenie rozumie się zdarzenie prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utraty, zmodyfikowania, nieuprawnionego ujawnienia lub dostępu do danych osobowych. Canna Gold Sp. z o.o. wdrożyła procedurę reagowania na takie incydenty, aby

zminimalizować ich skutki i spełnić obowiązki prawne związane z notyfikacją. Najważniejsze elementy tej procedury to:

- **Szybka identyfikacja i zgłoszenie incydentu:** Każdy pracownik, który stwierdzi lub podejrzewa naruszenie (np. zauważy, że laptop z danymi zaginął, system został zainfekowany wirusem, dokument papierowy trafił omyłkowo do nieuprawnionej osoby, nastąpił wyciek danych itp.), **niezwłocznie zgłasza ten fakt** Inspektorowi Ochrony Danych (jeśli powołany) lub bezpośrednio Zarządowi/koordynatorowi ds. ochrony danych. Szybkie zgłoszenie inicjuje odpowiednie kroki zaradcze.
- **Ocena incydentu i działania natychmiastowe:** Po zgłoszeniu zespół odpowiedzialny (IOD lub upoważnione osoby) dokonuje analizy zdarzenia – identyfikuje, jakie dane zostały naruszone, ilu osób dotyczy incydent, jakie mogą być konsekwencje naruszenia dla tych osób oraz czy naruszenie stwarza **ryzyko dla praw lub wolności osób fizycznych**. Równocześnie podejmowane są działania w celu powstrzymania naruszenia i zabezpieczenia danych (np. odłączenie zainfekowanego systemu od sieci, zmiana haseł, odzyskanie omyłkowo wysłanej wiadomości, przywracanie danych z backupu).
- **Notyfikacja organu nadzorczego (UODO):** Jeśli stwierdzimy, że naruszenie może powodować *ryzyko* naruszenia praw lub wolności osób fizycznych, **zgłaszamy naruszenie do Prezesa UODO** – *nie później niż w ciągu 72 godzin* od stwierdzenia naruszenia, zgodnie z art. 33 RODO. Zgłoszenie zawiera opis naruszenia, kategorie i przybliżoną liczbę osób, których dotyczy oraz zapisów danych, opis prawdopodobnych konsekwencji naruszenia, oraz opis środków podjętych lub proponowanych w celu zaradzenia naruszeniu. Jeśli zgłoszenie nie może być dokonane w ciągu 72 godzin, dołączamy wyjaśnienie przyczyn opóźnienia. Prowadzimy rejestr naruszeń, w którym odnotowujemy każde naruszenie, niezależnie od konieczności zgłoszenia do UODO.
- **Zawiadomienie osób, których dane dotyczą:** Jeśli oceniamy, że naruszenie może powodować *wysokie ryzyko* naruszenia praw lub wolności osób (np. wyciekły dane, których ujawnienie może narazić osoby na poważne konsekwencje finansowe, dyskryminację, kradzież tożsamości itp.), **niezwłocznie informujemy również te osoby** o zaistniałym naruszeniu. Komunikat do osób zawiera w prostym języku opis zdarzenia, wskazuje, jakie dane są dotknięte, opisuje możliwe konsekwencje oraz podaje, jakie środki zastosowaliśmy lub zalecamy osobie podjąć, by zminimalizować potencjalną szkodę (np. zmiana hasła, zastrzeżenie dokumentów). Informujemy również osobę o danych kontaktowych do naszego IOD lub punktu informacyjnego, gdzie może uzyskać więcej informacji. Nie musimy informować osób tylko wtedy, gdy

spełniony jest jeden z warunków z art. 34 ust. 3 RODO (np. wdrożyliśmy uprzednio odpowiednie środki bezpieczeństwa, które uczyniły dane niezrozumiałymi dla nieuprawnionych – np. silne szyfrowanie; podjęliśmy działania eliminujące wysokie ryzyko; lub wymagałoby to niewspółmiernie dużego wysiłku – wówczas wydajemy publiczny komunikat w środkach masowego przekazu).

- **Dokumentowanie i wnioski:** Każde naruszenie – niezależnie od skali – jest **udokumentowane** wewnętrznie (co się stało, kiedy, jakie działania podjęto, czy powiadomiono UODO i osoby). Analizujemy następnie przyczyny incydentu i wyciągamy wnioski, by na przyszłość uniknąć podobnych zdarzeń. Może to skutkować aktualizacją procedur, dodatkowymi szkoleniami dla personelu, wzmocnieniem zabezpieczeń technicznych itp. W ten sposób doskonalimy nasz system ochrony danych.

Spółka dysponuje gotowymi wzorcami zgłoszeń naruszeń do organu oraz szablonami zawiadomień dla osób, co pozwala przyspieszyć reakcję w sytuacji kryzysowej. Procedura zarządzania incydentami jest regularnie testowana (np. poprzez symulacje) i personel jest szkolony, jak się zachować w przypadku wykrycia incydentu. Dzięki temu ryzyko eskalacji szkód jest ograniczane, a obowiązki prawne w zakresie notyfikacji – wypełniane terminowo.

X. Rejestry i dokumentacja przetwarzania

Dla celów zapewnienia rozliczalności i lepszej organizacji, Spółka prowadzi wymaganą dokumentację procesów przetwarzania danych:

- **Rejestr Czynności Przetwarzania (RCP):** Jako Administrator danych, Canna Gold Sp. z o.o. utrzymuje RCP obejmujący wszystkie główne czynności przetwarzania danych osobowych w Spółce. W rejestrze tym zawarte są informacje takie jak: cel przetwarzania, kategorie osób, kategorie danych, podstawy prawne, opis kategorii odbiorców danych, ewentualne przekazywanie do państw trzecich, planowane terminy usunięcia poszczególnych kategorii danych, ogólny opis zabezpieczeń itp. Rejestr jest na bieżąco aktualizowany – każda nowa czynność przetwarzania przed jej rozpoczęciem jest w nim odnotowywana, a zakończone lub zmodyfikowane czynności są odpowiednio aktualizowane. Rejestr może być prowadzony w formie elektronicznej; udostępniamy go organowi nadzorczemu na żądanie zgodnie z art. 30 ust. 4 RODO.

- **Rejestr kategorii czynności (RKC):** Jeśli Spółka działałaby jako podmiot przetwarzający dane w imieniu innych administratorów (np. wykonując usługę na zlecenie, co obecnie nie ma miejsca), wówczas prowadzilibyśmy odrębny rejestr kategorii czynności wykonywanych dla każdego administratora. Obecnie Canna Gold pełni głównie rolę administratora własnych danych, zatem RKC nie występuje lub ma marginalne znaczenie.
- **Ewidencje upoważnień i odbiorców:** Wewnętrznie prowadzimy listę osób upoważnionych do przetwarzania danych (imię, nazwisko, rola, zakres upoważnienia, data nadania i ustania uprawnień). Ponadto dokumentujemy **ewidencję udostępnień danych** podmiotom zewnętrznym (komu, kiedy, jakie dane i na jakiej podstawie udostępniono) – co jest elementem wspierającym spełnienie obowiązku z art. 15 ust.1 lit. c RODO (informowanie osoby o odbiorcach jej danych).
- **Inne polityki i procedury:** Polityka ochrony danych osobowych jest elementem szerszego **systemu zarządzania ochroną danych** w Spółce. Towarzyszą jej szczegółowe procedury, o których była mowa wcześniej (np. procedura oceny skutków dla ochrony danych, procedura reagowania na incydenty, procedura obsługi żądań osób, procedura nadawania i odbierania upoważnień, polityka czystego biurka itp.). Dokumenty te wzajemnie się uzupełniają i wraz z Polityką tworzą spójną całość. W razie potrzeby stanowią one załączniki do niniejszej Polityki lub odrębne regulacje wewnętrzne.
- **Dowody spełnienia obowiązków:** Spółka przechowuje dowody na wykonanie kluczowych obowiązków ochrony danych – np. kopie klauzul informacyjnych przekazanych osobom (lub treści komunikatów informacyjnych stosowanych na stronie internetowej), zgody osób (o ile były zbierane – wraz z informacją kiedy i jak zostały udzielone lub wycofane), potwierdzenia wysłania zawiadomień o naruszeniach, raporty z przeprowadzonych szkoleń RODO dla pracowników, protokoły z audytów wewnętrznych itp. Wszystko to ma na celu wykazanie ewentualnej zgodności z przepisami w przypadku kontroli lub zapytania ze strony organu nadzorczego.

XI. Szkolenia i podnoszenie świadomości

Spółka dokłada starań, aby wszyscy pracownicy i współpracownicy mieli odpowiednią wiedzę na temat zasad ochrony danych osobowych. Realizujemy to poprzez:

- **Szkolenia wstępne:** Nowo zatrudnione osoby odbywają szkolenie lub instruktaż z zakresu ochrony danych przed dopuszczeniem do przetwarzania danych. Omawiamy na nim podstawy prawne, zasady RODO, wewnętrzne procedury

oraz odpowiedzialność pracowników. Każda taka osoba potwierdza zapoznanie się z Polityką i zobowiązuje się jej przestrzegać (podpisanie oświadczenia o zapoznaniu się z regulacjami ochrony danych osobowych).

- **Szkolenia okresowe:** Co pewien czas (np. raz do roku lub częściej w razie istotnych zmian przepisów) organizujemy szkolenia przypominające/aktualizujące dla całego personelu. Poruszane są na nich m.in. najnowsze wytyczne organu nadzorczego, wnioski z audytów, omówienie incydentów które miały miejsce (aby wyciągnąć naukę na przyszłość), nowe procedury lub zmiany w Polityce.
- **Materiały informacyjne:** Udostępniamy pracownikom materiały takie jak poradniki, infografiki, check-listy dotyczące bezpiecznej pracy z danymi (np. jak rozpoznawać phishing, jak obsługiwać prawa osób, jak zabezpieczać dokumenty). W siedzibie, w strefach pracowniczych, umieszczone są plakaty przypominające o zasadach ochrony danych (np. „Sprawdź uprawnienia przed udostępnieniem danych przez telefon").
- **Testy i weryfikacja wiedzy:** Po szkoleniach przeprowadzamy krótkie testy wiedzy lub quizy, aby upewnić się, że kluczowe zagadnienia zostały zrozumiane. Jeśli wynik testu jest niezadowalający, dana osoba kierowana jest na dodatkowe szkolenie.
- **Polityka otwartych drzwi:** Inspektor Ochrony Danych (jeżeli powołany) lub osoba pełniąca jego obowiązki jest dostępna dla pracowników w razie pytań lub wątpliwości związanych z ochroną danych. Zachęcamy personel do konsultowania wszelkich niejasnych sytuacji – lepiej zapytać zawczasu, niż popełnić błąd skutkujący naruszeniem. Tworzymy atmosferę, w której zgłaszanie problemów (np. zauważonych potencjalnych słabości zabezpieczeń) jest mile widziane i nie spotyka się z negatywnymi konsekwencjami.
- **Podnoszenie świadomości na co dzień:** Ochrona danych jest stałym elementem **kultury organizacyjnej** Spółki. Kierownictwo daje dobry przykład, przestrzegając zasad (tone at the top). Regularnie w komunikacji wewnętrznej przypominamy o istotnych kwestiach (np. w okresie urlopowym – o niepozostawianiu wrażliwych dokumentów na biurkach, przed świętami – o ostrożności na ataki phishing podszywające się pod kartki świąteczne, itp.). Dzięki temu bezpieczeństwo informacji pozostaje w świadomości pracowników, a nie jedynie w dokumentach.

Realizacja powyższych działań szkoleniowych sprzyja budowaniu kompetentnego zespołu, który prawidłowo reaguje w sytuacjach związanych z ochroną danych osobowych. Wszyscy pracownicy rozumieją, że ochrona danych to **wspólna odpowiedzialność**, a nie tylko zadanie działu prawnego czy IT.

XII. Postanowienia końcowe

Przegląd i aktualizacja Polityki: Niniejsza Polityka Ochrony Danych Osobowych podlega regularnym przeglądom. Co najmniej raz w roku (lub częściej, w razie istotnych zmian okoliczności) dokonuje się jej **oceny i aktualizacji**. Uwzględniane są przy tym zmiany w przepisach prawa, nowe wytyczne organu nadzorczego, zmiany organizacyjne w Spółce, postęp technologiczny czy pojawienie się nowych zagrożeń dla bezpieczeństwa. W szczególności, jeśli w otoczeniu prawnym wejdą w życie nowe regulacje dotyczące ochrony danych lub orzeczenia/interpretacje wpływające na nasze obowiązki – Polityka zostanie zweryfikowana pod tym kątem i odpowiednio zmodyfikowana. Za aktualizację Polityki odpowiada wyznaczona osoba (Inspektor Ochrony Danych lub inny członek kierownictwa). Wszelkie zmiany Polityki są **komunikowane pracownikom** (np. poprzez rozesłanie zaktualizowanego tekstu i omówienie zmian na zebraniu) oraz wdrażane w praktyce. W razie znaczących zmian, osoby, których dane dotyczą (np. klienci) zostaną poinformowane, jeśli zmiana Polityki miałaby wpływ na sposób przetwarzania ich danych.

Obowiązywanie Polityki: Polityka wchodzi w życie z dniem zatwierdzenia przez Zarząd Spółki i obowiązuje do odwołania lub zastąpienia nową wersją. Wszelkie wcześniejsze wewnętrzne regulacje dotyczące bezpieczeństwa informacji lub ochrony danych, o ile istniały, zostają z dniem wdrożenia niniejszej Polityki zintegrowane z jej postanowieniami lub uchylone – tak, aby uniknąć sprzeczności i rozproszenia wymogów.

Odpowiedzialność za naruszenie zasad: Nieprzestrzeganie postanowień niniejszej Polityki przez pracowników lub współpracowników Spółki może skutkować konsekwencjami dyscyplinarnymi, a w skrajnych przypadkach – odpowiedzialnością prawną (np. gdy umyślne działanie pracownika doprowadzi do poważnego naruszenia ochrony danych, Spółka może podjąć kroki prawne). Każdy członek personelu jest zobowiązany do raportowania incydentów i podejrzeń naruszeń bez obawy przed negatywnymi następstwami – promujemy zgłaszanie problemów, gdyż służy to wspólnemu bezpieczeństwu.

Kontakt w sprawach ochrony danych: Wszelkie pytania, uwagi lub wnioski dotyczące niniejszej Polityki lub ogólnie ochrony danych osobowych w Canna Gold Sp. z o.o. można kierować do wyznaczonej osoby kontaktowej. Jeśli powołano Inspektora Ochrony Danych, jego dane kontaktowe są dostępne w klauzulach informacyjnych i na stronie internetowej Spółki. W przeciwnym razie prosimy kontaktować się z Administratorem danych pod adresem e-mail: **[adres email Spółki]** lub pisemnie na

adres siedziby Spółki. Udzielimy odpowiedzi najszybciej jak to możliwe, nie później niż w terminach przewidzianych prawem.

Polityka Ochrony Danych Osobowych Canna Gold Sp. z o.o. stanowi wyraz naszego zaangażowania w poszanowanie prywatności i ochronę danych osobowych. Zarząd Spółki w pełni popiera niniejszy dokument i zapewnia środki niezbędne do jego realizacji. Wszyscy pracownicy zostali zapoznani z treścią Polityki i zobowiązani do jej przestrzegania. Spółka będzie dążyć do stałego podnoszenia standardów bezpieczeństwa informacji, tak aby utrzymać zaufanie klientów, partnerów oraz spełnić wymagania prawa w zakresie ochrony danych osobowych.

Ostatnia aktualizacja Polityki: ***01.01.2025r.***