Polityka przetwarzania i ochrony danych osobowych w spółce PKLD Sp. z o.o.

Spis treści

Polityka przetwarzania i ochrony danych osobowych w spółce PKLD Sp. z o.o.

1. Cel Polityki i podstawy prawne

Niniejsza Polityka ustanawia zasady przetwarzania i ochrony danych osobowych w Spółce PKLD Sp. z o.o. oraz sposoby realizacji praw przysługujących podmiotom danych, zgodnie z wymaganiami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, dalej: „RODO") oraz Ustawy z dn. 10 maja 2018r. o ochronie danych osobowych (dalej „Ustawa").

2. Administrator Danych

Administratorem danych osobowych jest PKLD Sp. z o.o. z siedzibą w Bielawie, ul. Wspólna 71 05-520 Bielawa, reprezentowana przez Zarząd (dalej: „Administrator" lub „Spółka").

3. Zakresy odpowiedzialności

Każda osoba, która w związku z wykonywaniem czynności w imieniu lub na polecenie Administratora uzyska dostęp do jakichkolwiek danych osobowych, a więc informacji o zidentyfikowanej lub możliwejdo zidentyfikowania osobie fizycznej, zobowiązana jest do przetwarzania i do ochrony tych danych zgodnie z RODO, Ustawą i postanowieniami niniejszej Polityki przez cały okres zatrudnienia/współpracy, a także po jego ustaniu, bez względu ma formę zatrudnienia lub współpracy. Każda osoba przetwarzająca dane osobowe w związku z pracą wykonywaną w Spółce lub na rzecz Spółki ponosi odpowiedzialność (dyscyplinarną, administracyjną i karną) za wynikające z tego przetwarzania naruszenie obowiązków lub przepisów prawa.

W Spółce określa się niżej opisane obszary odpowiedzialności za ochronę danych.

3.1. Prezes Zarządu

Prezes Zarządu jest zobowiązany do:

- zapewnienia zgodności przetwarzania danych osobowych z obowiązującymi przepisami prawa;
- zapewnienia warunków technicznych i organizacyjnych pozwalających na przetwarzanie danych osobowych zgodnie z wymaganiami RODO, w tym zapewnienie odpowiedniego stopnia bezpieczeństwa danych osobowych przetwarzanych w zasobach teleinformatycznych;
- zapewnienia realizacji praw osób, których dane są przetwarzane w Spółce;
- nadawanie upoważnień do przetwarzania danych osobowych;
- monitorowania przestrzegania RODO, innych przepisów o ochronie danych osobowych oraz Polityki, w tym prowadzenie kontroli związanych z operacjami przetwarzania danych;
- współpracy z organem nadzorczym w ramach wykonywanych zadań;
- decydowania o celach i sposobach przetwarzania danych;
- uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych;
- oceny kontrahentów (obecnych i potencjalnych), pod kątem dawanych przez nich gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych.

3.2. Pracownik od spraw administracyjnych

Pracownik od spraw administracyjnych jest zobowiązany do:

- prowadzenia rejestru osób upoważnionych do przetwarzania danych osobowych;
- prowadzenia rejestru czynności przetwarzania (dla procesów, w których Spółka jest administratorem) i rejestru wszystkich kategorii przetwarzania danych osobowych przetwarzania (dla procesów, w których Spółka jest podmiotem przewarzającym);
- zarządzania obsługą wniosków/żądań osób, dotyczących wykonywania ich praw w związku z przetwarzaniem danych osobowych;
- wsparcia Prezesa Zarządu w realizacji czynności opisanych w pkt. 3.1.

3.3. Osoba zajmująca się obsługą informatyczną

Osoba zajmująca się obsługą informatyczną jest zobowiązana do:

- udziału w prowadzeniu oceny ryzyka dla operacji wymagających przetwarzania danych osobowych w zasobach teleinformatycznych i konfiguracji systemów informatycznych wykorzystywanych przez Spółkę w sposób zapewniający stopień bezpieczeństwa odpowiadający ryzyku;
- opracowania i aktualizacji Wykazu zabezpieczeń, w tym odpowiednich procedur związanychz tworzeniem kopii zapasowych (back'up), retencją danych;
- wdrożenia i utrzymywania narzędzi informatycznych, które są niezbędne do skutecznego wykonywania przez Administratora praw (żądań) podmiotów danych oraz wymogów przepisów o ochronie danych osobowych;
- zapewnienia zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich - w razie wystąpienia incydentu prowadzącego do naruszenia ochrony danych.

3.4. Pracownik[1]

Pracownik jest zobowiązany do:

- zapoznania i postępowania zgodnie z wymaganiami RODO, Ustawy i niniejszej Polityki;
- zachowania w tajemnicy danych osobowych przetwarzanych w związku z wykonywaniem obowiązków służbowych oraz zachowania w tajemnicy sposobów zabezpieczania danych;
- wykonywania operacji przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem;
- przyjmowania i zgłaszania do Pracownika od spraw administracyjnych wpływających wniosków/żądań osób, dotyczących wykonywania ich praw w związku z przetwarzaniem danych osobowych;
- uniemożliwienia osobom nieupoważnionym dostępu do danych osobowych, rozumianego również jako nieujawnianie haseł do zasobów teleinformatycznych, w których przetwarzane są dane osobowe;
- niezwłocznego zgłaszania do Pracownika od spraw administracyjnych wszelkich nieprawidłowości związanych z przetwarzaniem i ochroną danych osobowych.

4. Organizacja przetwarzania danych w Spółce

W przetwarzaniu danych osobowych w Spółce mogą uczestniczyć jedynie osoby posiadające stosowne upoważnienie nadane przez Administratora.

4.1. Osoby upoważnione

Wszyscy Pracownicy, którym - w związku z wykonywaniem obowiązków służbowych u Administratora – potrzebny jest dostęp do danych osobowych, zobowiązani są zapoznać się z wymaganiami RODO, Ustawy i zasadami zawartymi w niniejszej Polityce oraz złożyć oświadczenie o zachowaniu w tajemnicy

[1] Pracownik - osoba zatrudniona w PKLD Sp. z o.o. na umowę o pracę lub osoba fizyczna świadcząca usługi na rzecz Spółki na podstawie umowy cywilnoprawnej.

wszelkich danych osobowych oraz sposobów ich zabezpieczania. Administrator podejmuje działania w celu zapewnienia, by każda osoba, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie Administratora. Wzór upoważnienia wraz z treścią oświadczenia o zachowaniu w tajemnicy danych osobowych i sposobów ich zabezpieczania stanowi Załącznik nr 1.

Upoważnienie do przetwarzania danych jest ważne przez okres świadczenia pracy/usług przez osobę upoważnioną lub do jego odwołania. W przypadku, gdy w związku z realizacją obowiązków służbowych Administrator zleca Pracownikowi czynności wymagające przetwarzania danych osobowych w zakresie innym, niż zawarty na upoważnieniu, konieczna jest jego aktualizacja (uzupełnienie). Wszystkie upoważnienia przechowuje się przez cały czas pracy Pracownika lub do czasu wygaśnięcia roszczeń wynikających z odrębnych umów o świadczenie usług. Upoważnienia są wydawane w dwóch egzemplarzach – jeden otrzymuje Pracownik, a drugi jest przechowywany w aktach osobowych. Pracownik od spraw administracyjnych prowadzi i aktualizuje rejestr osób upoważnionych do przetwarzania danych osobowych, wg wzoru zawartego w Załączniku nr 2.

4.2. Szkolenia

Pracownicy są szkoleni z zasad odnoszących się do przetwarzania i ochrony danych osobowych, przed dopuszczeniem do pracy. Szkolenie jest przeprowadzone przez wskazaną przez Administratora osobę. Dopuszcza się również możliwość zapoznania Pracownika z zasadami ochrony danych osobowych poprzez udostępnienie mu w formie elektronicznej lub papierowej właściwych przepisów prawa i dokumentacji. Pracownicy Administratora i wszystkie osoby, które będą przetwarzać dane osobowe na jego polecenie zobowiązani są do zapoznania się z zasadami ochrony danych osobowych zawartymiw RODO, Ustawie i niniejszej Polityce. Wszystkie osoby, które przetwarzają dane osobowe napolecenie Administratora potwierdzają fakt zapoznania się z ww. dokumentami, poprzez złożenie podpisu na oświadczeniu o nieujawnianiu danych osobowych i sposobów ich zabezpieczania, którego treść znajduje się na formularzu upoważnienia.

4.3. Zabezpieczenie danych osobowych przetwarzanych w formie papierowej

Dane osobowe są przechowywane w sposób zapewniający odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem, przypadkową utratą, zniszczeniem lub uszkodzeniem.

Przy przetwarzaniu danych osobowych w formie papierowej stosuje się zasadę „czystego biurka”, rozumianą jako zakaz pozostawiania dokumentów zawierających dane osobowe w miejscu ogólnie dostępnym oraz obowiązek przechowywania takich dokumentów w meblach biurowych zamykanych na klucz, w pomieszczeniach o ograniczonej możliwości przebywania osób nieupoważnionych. Stosuje się również zasadę „ograniczonego dostępu” - osoby nieupoważnione mogą przebywać w tych pomieszczeniach wyłącznie pod opieką osoby upoważnionej.

Niszczenie materiałów zawierających dane osobowe odbywa się przy użyciu niszczarek ścinkowych. W przypadku, gdy konsekwencją takiego zniszczenia jest usunięcie podmiotu danych z bazy administratora, przed zniszczeniem należy się upewnić, czy spełnione są warunki wynikające z pkt. 6.3 poniżej.

4.4. Zabezpieczenie danych osobowych przetwarzanych w formie elektronicznej

Przy przetwarzaniu danych osobowych w formie elektronicznej należy stosować zabezpieczenia uniemożliwiające osobom nieupoważnionym jakiekolwiek czynności na plikach zawierających dane.W tym celu Administrator zobowiązany jest zapewnić, jeżeli jest to tylko możliwe, minimalne sposoby zabezpieczenia komputerów firmowych poprzez:

- ustawienie hasła startowego podczas uruchamiania komputera;
- ochronę dostępu do kont użytkowników systemu operacyjnego, gdzie są przechowywane dane,przy pomocy indywidualnego minimum 8-znakowego hasła dostępu, zawierającego duże i małe

litery, cyfry i znaki specjalne. Hasło dostępu nie może zawierać żadnych informacji mogących kojarzyć się z użytkownikiem danego komputera. Hasło ulega zmianie nie rzadziej niż co 30 dni;

- zapewnienie indywidualnych kont użytkownika systemu operacyjnego, w przypadku używania komputera przez więcej niż jedną osobę. Każde konto chronione jest hasłem założonym zgodnie z zasadami opisanymi w punkcie poprzednim;
- uniemożliwiający osobom postronnym zapoznanie się z hasłem;
- uruchomienie wygaszacza ekranu w przypadku bezczynności w pracy dłuższej niż 3 minuty.Przy wznowieniu pracy systemu, użytkownik ponownie podaje hasło na wyświetlanym ekranie logowania;
- blokowanie widoku ekranu w przypadku odejścia od komputera (np. poprzez równoczesne naciśnięcie klawiszy Ctrl + Alt + Del i wybranie opcji „Zablokuj" lub równoczesne naciśnięcie klawiszy ⊞ + L);
- ustawienie monitorów komputerów użytkowanych przez Pracowników w sposóbuniemożliwiający osobom nieuprawnionym zapoznanie się z treścią wyświetlanych informacji;
- szyfrowanie danych na dysku.

W przypadku konieczności przeprowadzenia przez podmiot zewnętrzny prac serwisowychna komputerze zawierającym dane osobowe, zlecenie usługi musi zawierać stosowne regulacje zobowiązujące podmiot serwisujący do zapewnienia właściwej ochrony danych osobowych.

W przypadku konieczności utylizacji / likwidacji / odsprzedaży komputera, przy użyciu którego przetwarzano dane osobowe, przed dokonaniem tych czynności należy odpowiednio przygotować komputer tj. należy skutecznie usunąć z niego wszelkie dane osobowe. Czynność tę potwierdza się protokołem.

Przed przesłaniem pliku zawierającego dane osobowe do innej, upoważnionej osoby lub przed zapisaniem pliku na elektronicznym nośniku informacji należy go zabezpieczyć przy użyciu algorytmu szyfrującego min. AES 256 8-znakowym hasłem zawierającym duże i małe litery, cyfry i znaki specjalne. Po potwierdzeniu przez odbiorcę otrzymania zabezpieczonego pliku lub elektronicznego nośnika informacji, nadawca przekazuje mu hasło (o ile to możliwe - innym kanałem łączności, np. połączenie telefoniczne, sms).

Wykorzystywane przez Administratora systemy i zasoby teleinformatyczne podlegają systematycznemu sprawdzeniu pod kątem spełnienia wymagań bezpieczeństwa.

Systemy informatyczne, w których przetwarzane są dane osobowe posiadają zdolność do zapewnienia poufności, integralności i dostępności oraz zdolność do szybkiego przywrócenia dostępności w razieincydentu fizycznego lub technicznego.

Szczegóły dotyczące konfiguracji, zabezpieczeń i funkcjonowania systemów i programów informatycznych wykorzystywanych przez Spółkę w związku z prowadzoną przez nią działalnością, określone są w odrębnej procedurze.

4.5. Kontrola wewnętrzna

W celu weryfikacji zgodności przetwarzania danych osobowych z zasadami opisanymi w RODO, Ustawie i niniejszej Polityce, Administrator lub wskazana przez niego osoba może przeprowadzać wewnętrzne kontrole. O planie przeprowadzenia kontroli Administrator informuje z tygodniowym wyprzedzeniem. Pracownicy kontrolowanego obszaru są zobowiązani do udzielenia odpowiedzi na pytania kontrolującego. Z kontroli sporządza się protokół, którego treść jest przekazywana do wiadomości Administratora.

Administrator prowadzi również cykliczną ocenę ryzyka naruszenia praw i wolności osób fizycznychw związku z przetwarzaniem ich danych osobowych oraz podejmuje działania w celu minimalizacji ryzyka.

Pracownik od spraw administracyjnych co najmniej raz w każdym roku kalendarzowym przeprowadza i dokumentuje protokołem weryfikację zasobów danych osobowych prowadzonych zarówno w formie papierowej, jak i elektronicznej, obejmującą:

- sprawdzenie, czy zostały usunięte dane osobowe, dla których upłynął okres przechowywania wynikający z przepisów prawa;
- sprawdzenie, czy w odniesieniu do danych osobowych, których czas przechowywania nie został określony przez właściwe przepisy prawa, nadal istnieje podstawa prawna oraz cel przetwarzania.

5. Zasady przetwarzania danych

Administrator, przy przetwarzaniu danych osobowych kieruje się zasadami opisanymi poniżej.

5.1. Zasada „zgodności z prawem, rzetelności i przejrzystości”

Dla każdego z procesów realizowanych w Spółce wskazuje się odpowiadającą mu podstawę prawną dla przetwarzania danych osobowych, która jest ujęta w rejestrze czynności przetwarzania. Zasada wymaga, by dane osobowe były przetwarzane na podstawie spełnienia przynajmniej jednego z warunków wymienionych w art. 6 pkt. 1 RODO.

Podmiotowi danych podaje się informacje dotyczące sposobu przetwarzania dotyczących go danych, zgodnie z art. 13 RODO (gdy dane są zbierane bezpośrednio od podmiotów danych) lub art. 14 RODO (gdy dane są pozyskiwane w inny sposób niż bezpośrednio od podmiotów danych) w postaci klauzuli informacyjnej Dla każdego z procesów realizowanych w Spółce stosuje się osobną klauzulę informacyjną.

W przypadku, gdy przetwarzanie danych odbywa się na podstawie zgody, Administrator jest zobowiązany wykazać każdym czasie, że zgodę taką pozyskał. Osoba, której dane dotyczą ma zapewnioną możliwość wycofania zgody. Administrator odnotowuje w systemie daty złożeniai wycofania zgody.

5.2. Zasada „ograniczenia celu”

Zasada wymaga, by dane były zbierane w konkretnych, prawnie uzasadnionych celach. Administrator stosuje tę zasadę określając cel i zakres przetwarzania danych dla poszczególnych procesów.

5.3. Zasada „minimalizacji danych”

Zasada wymaga ograniczenia zakresu zbierania danych wyłącznie do tych kategorii danych, które są niezbędne do osiągnięcia celów przetwarzania. Administrator stosuje tę zasadę określając zakresy dla poszczególnych procesów.

5.4. Zasada „prawidłowości”

Zasada wymaga bieżącego sprawdzania i w razie potrzeby uaktualniania danych oraz usuwania lub sprostowania danych nieprawidłowych. Administrator realizuje tę zasadę przy każdym kontakciez podmiotem danych.

5.5. Zasada „ograniczenia przechowywania”

Zasada wymaga, by forma przechowywania danych osobowych umożliwiała identyfikację podmiotu danych jedynie przez czas niezbędny do realizacji celów, w których te dane są przetwarzane. Po upływie

okresu przyjętego dla przetwarzania danych, Administrator anonimizuje lub usuwa dane ze swoich systemów wraz z ustaniem celu przetwarzania lub po upływie czasu związanego z obsługą roszczeń.

5.6. Zasada „integralności i poufności”

Zasada wymaga stosowania odpowiednich środków technicznych i organizacyjnych zapewniających ochronę przed niezgodnym z prawem przetwarzaniem lub przypadkową utratą, zniszczeniem lub uszkodzeniem.

5.7. Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

Administrator wdrożył odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia konkretnego celu przetwarzania. Przez zobowiązanie to rozumie się ograniczanie do niezbędnego minimum ilości zbieranych danych osobowych, zawężanie zakresu ich przetwarzania oraz określanie możliwie krótkich okresów przetwarzania.

Administrator odpowiada za zarządzanie zmianą w procesie realizowanym lub planowanym. Pracownik od spraw administracyjnych na etapie projektowania zmiany do aktywnego procesu lub na etapie przygotowania do wdrożenia nowego procesu, jest zobowiązany przeprowadzić analizę zgodności z obowiązującymi przepisami prawa w zakresie ochrony danych osobowych oraz uczestniczyć w ocenie ryzyka naruszenia praw lub wolności osób, a także - jeśli to konieczne (w przypadku oszacowania ryzyka na poziomie wysokim) – dokonać oceny skutków planowanego procesu przetwarzania dla ochrony danych osobowych.

Biorąc pod uwagę wyniki przeprowadzonej oceny ryzyka oraz wdrożone już środki technicznei organizacyjne, Administrator podejmuje decyzję o akceptacji tego ryzyka lub wdraża dodatkowe środki w celu jego obniżenia do akceptowalnego poziomu.

Jeśli mimo zastosowanych środków technicznych i organizacyjnych proces przetwarzania powoduje bardzo duże prawdopodobieństwo wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych, konieczne jest skonsultowanie procesu z organem nadzorczym.

Każda zmiana w procesach przetwarzania wymaga odnotowania w dokumentacji wewnętrznej (w tymwe właściwych rejestrach prowadzonych dla czynności przetwarzania danych osobowych).

6. Prawa osób – procedura obsługi żądań

Administrator utrzymuje stosowne środki, by terminowo, w sposób zwięzły, zrozumiały i łatwo dostępny udzielić osobie, której dane dotyczą informacji, o których mowa w art. 13 i 14 RODO, oraz prowadzić z nią wszelką komunikację w sprawie przetwarzania, na mocy art. 15–22 i 34 RODO. Jako zasadę przyjmuje się, że informacji (odpowiedzi na żądanie) udziela się na piśmie, chyba że żądanie wpłynęło w formie elektronicznej, wówczas – elektronicznie.

Każdy Pracownik, w przypadku odebrania wniosku/żądania osoby, dotyczącego wykonywania jej praw w związku z przetwarzaniem danych osobowych zobowiązany jest do niezwłocznego przekazania godo Pracownika od spraw administracyjnych. W przypadku przyjęcia zgłoszenia żądania w trakcie połączenia telefonicznego, Pracownik zwraca się z prośbą do podmiotu danych o przesłanie zgłoszenia na adres rodo@jumpy.pl.

Pracownik od spraw administracyjnych odnotowuje w rejestrze żądań wszelkie możliwe informacje dot. żądania (numer porządkowy żądania, datę otrzymania żądania, imię i nazwisko podmiotu danych zgłaszającego żądanie, informację, czy jest to pierwsze czy kolejne zgłaszającego podmiotu danych, krótki opis, czego dotyczy żądanie (prawo dostępu, prawo ograniczenia danych, sprostowania, inne).

Przed realizacją żądania należy dokonać analizy, czy dane prawo przysługuje w przypadku przetwarzania danych na określonej podstawie prawnej. O ile to możliwe, Pracownik od spraw administracyjnych wprowadza zmiany wynikające z żądania i udziela stosownej odpowiedzi podmiotowi danych.

W sytuacji powierzenia danych podmiotom przetwarzającym lub udostępnienia danych innym administratorom danych, należy ich powiadamiać o każdym sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych, które było wynikiem realizacji wniosku podmiotu danych.

Najpóźniej w ciągu miesiąca od otrzymania żądania, udziela się podmiotowi danych informacji zwrotnejlub – w przypadku przewidywanego opóźnienia – uzasadnia się przyczynę zwłoki.

Informacje podawane na mocy artykułów 13-22 i 34 RODO są wolne od opłat. Jeżeli żądania osoby,której dane dotyczą są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swójustawiczny charakter, administrator może pobrać opłatę lub odmówić podjęcia działań w związku z tematem, o ile może wykazać nieuzasadniony lub nadmierny charakter żądania.

Administrator prowadzi Rejestr żądań, którego wzór stanowi Załącznik nr 3 do niniejszej Polityki.

6.1. Prawo dostępu

Dane osobowe przetwarzane są w uporządkowanych bazach Administratora, pozwalających na szybkie wyszukanie i udzielenie podmiotowi danych informacji, czy przetwarza jego dane osobowe oraz udzielenie informacji o celu przetwarzania, kategoriach danych osobowych, odbiorcach danych,o planowanym okresie ich przechowywania (lub kryteriach jego ustalania). W przypadku, gdy podmiot danych zażąda dostępu do jego danych osobowych podlegających przetwarzaniu u Administratora, dostarczana jest mu kopia danych, chyba że mogłoby to niekorzystnie wpływać na prawa i wolności innych osób.

6.2. Prawo do sprostowania danych

Sprostowanie danych oznacza korektę danych, które podmiot danych uważa za nieprawdziwe lub nieprawidłowe. W przypadku, gdy podmiot danych skieruje do Administratora żądanie sprostowania danych lub uzupełnienia niekompletnych danych, upoważniony Pracownik wykonuje tę czynność, pilnując, by zakres uzupełnianych danych nie wykraczał poza zakres niezbędny do celu przetwarzaniadanych w procesie.

6.3. Prawo do usunięcia danych („prawo do bycia zapomnianym")

Podmiot danych ma prawo do żądania usunięcia danych w przypadku, gdy dane te nie są już niezbędne do celów, w których zostały zebrane, gdy wycofał zgodę na przetwarzanie danych (a nie ma innej postawy prawnej przetwarzania), wniósł sprzeciw przetwarzania danych w związku ze swoją szczególną sytuacją albo wobec przetwarzania danych dla celów marketingowych lub wystąpiły inne sytuacje opisane w art.17 RODO. W takich przypadkach Pracownik od spraw administracyjnych dokonuje usunięcia danych z baz i systemów oraz podejmuje czynności wobec podmiotów, którym te dane przekazano, w celu poinformowania ich o otrzymanym żądaniu usunięcia. Żądanie pozostaje niezrealizowane w przypadku, gdy inny przepis prawa nakazuje przetwarzanie danych osobowych orazw sytuacji, gdy przetwarzanie danych jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń.

6.4. Prawo do ograniczenia przetwarzania

Administrator uznaje prawo podmiotu danych do żądania ograniczenia przetwarzania danych, gdy kwestionuje prawidłowość przetwarzania danych. Ograniczone dane można przetwarzać, z wyjątkiem przechowywania, za zgodą podmiotu danych lub w celu ustalenia dochodzenia lub obrony roszczeń.

6.5. Prawo do przenoszenia danych

Administrator wdraża środki techniczne pozwalające na realizację prawa podmiotu danych do przenoszenia danych. Prawo to może być wykonane wyłącznie wtedy, gdy dane przetwarzanona podstawie zgody, ich przetwarzanie było niezbędne do wykonania umowy lub przetwarzanie odbywało się w sposób zautomatyzowany. Prawo to obejmuje wyłącznie dane przy użyciu systemów informatycznych (nie obejmuje papierowych zbiorów danych).

Dane muszą być przekazywane w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego.

6.6. Prawo do sprzeciwu

Administrator uznaje prawo podmiotu danych do wniesienia sprzeciwu wobec przetwarzania jego danych osobowych, pozyskanych na podstawie prawnie uzasadnionego interesu Po takim sprzeciwie administrator nie może przetwarzać już tych danych, chyba że wykaże on istnienie ważnych, prawnie usprawiedliwionych podstaw do przetwarzania danych, nadrzędnych wobec interesów, praw i wolności podmiotu danych lub podstaw do ustalenia, dochodzenia lub obrony roszczeń. W przypadku potwierdzenia zasadności sprzeciwu wniesionego przez osobę, której dane dotyczą, Właściciel procesu, we współpracy z Osobą zajmującą się obsługą informatyczną, zobowiązany jest zaprzestaćprzetwarzania danych osobowych objętych takim sprzeciwem.

6.7. Prawo do wniesienia skargi do organu nadzorczego

Podmiot danych ma prawo do wniesienia skargi do organu nadzorczego. Administrator jest zobowiązany do współpracy i udzielania odpowiedzi organowi nadzorczemu.

6.8. Profilowanie

Profilowanie to dowolna forma zautomatyzowanego przetwarzania danych osobowych, polegająca na ich wykorzystaniu w celu oceny niektórych czynników osobowych, a w szczególności do analizy lub prognozy aspektów dotyczących działań tej osoby, jej sytuacji ekonomicznej, stanu zdrowia, wiarygodności, lokalizacji lub przemieszczania się. Administrator, za art. 22 RODO, uznaje prawo każdego podmiotu danych, by decyzje wobec niego nie były podejmowane wyłącznie w oparciuo zautomatyzowane przetwarzanie danych osobowych, które mogłoby prowadzić do powstania wobectej osoby skutków prawnych. W przypadku konstruowania procesu profilowania, Administrator zapewnia zaangażowanie podmiotu danych w proces decyzyjny. Wyjątek dla decyzji opierającej się wyłącznie na zautomatyzowanym przetwarzaniu stanowią następujące sytuacje:

- decyzja jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą a Administratorem;
- decyzja jest dozwolona prawem Unii Europejskiej lub prawem krajowym, które przewiduje właściwe środki ochrony praw, wolności i uzasadnionych interesów osoby, której dane dotyczą;
- decyzja opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

7. Przekazywanie danych osobowych innym odbiorcom/podmiotom przetwarzającym

Spółka przyjmuje do stosowania zasady doboru i weryfikacji podmiotów przetwarzających dane na jej rzecz, w celu uzyskania gwarancji wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa ochrony danych osobowych. Przed przystąpieniem do współpracy, w ramach której będzie dochodziło do przekazania danych osobowych, Spółka sprawdza czy potencjalny kontrahent wdrożył wymagania RODO, w tym:

- czy podmiot ten wdrożył dokumentację przetwarzania danych zgodną z RODO;

- czy prowadzi i utrzymuje rejestry, o których mowa w art. 30 RODO;
- czy zapewnia, identyfikuje i weryfikuje podstawy prawne przetwarzania danych;
- czy spełnia obowiązki informacyjne względem osób, których dane przetwarza;
- czy zapewnia obsługę praw podmiotów danych, realizując otrzymane w tym zakresie żądania;
- czy zapewnia, by dane osobowe były przetwarzane wyłącznie przez upoważnione osoby,w zakresie danego im polecenia przetwarzania danych;
- czy zapewnia ochronę danych i podejmuje środki ochrony, zgodnie z art.32 RODO;
- czy posiada procedury zapewniające zgłaszanie naruszeń organowi nadzorczemu oraz zawiadamianie osób, których dane naruszono;
- czy weryfikuje podmioty, którym powierza dane, pod kątem spełnienia przez nie wymagań RODO.

Administrator prowadzi rejestr ujawnień danych innym odbiorcom według wzoru stanowiącego Załącznik nr 4.

7.1. Współadministrowanie danymi osobowymi

W przypadku zaistnienia procesu wymagającego wspólnego, z innym administratorem, ustalania celówi sposobów przetwarzania, Spółka wraz z tym podmiotem określa w zakresy odpowiedzialności, w tym, w odniesieniu do wykonywania przez podmiot danych przysługujących jej praw oraz ich obowiązków informacyjnych wynikających z art. 13 i art.14 RODO, a także wskazuje się punkt kontaktowy dla podmiotów danych.

7.2. Powierzenie przetwarzania danych osobowych

W przypadku, gdy w związku z realizacją umowy biznesowej zachodzi konieczność powierzenia innemu podmiotowi danych osobowych, których Administratorem jest Spółka, a także w przypadku, gdy to druga strona planuje powierzenie danych osobowych do Spółki, strony zobowiązane są do zawarcia umowy powierzenia, w formie pisemnej lub elektronicznej, w której określają:

- przedmiot i czas trwania przetwarzania,
- rodzaj danych osobowych
- kategorie osób, których dane dotyczą,
- obowiązki i prawa stron.

Umowa powinna również obejmować następujące zasady:

- przetwarzanie danych osobowych wyłącznie na udokumentowane polecenie Administratora;
- zapewnienie, by osoby upoważnione do przetwarzania danych osobowych zobowiązały siędo zachowania tajemnicy;
- oświadczenie o podjęciu wszelkich środków wymaganych na mocy art. 32 RODO;
- przestrzeganie warunków korzystania z usług innego podmiotu przetwarzającego;
- zobowiązanie do pomocy administratorowi w wywiązaniu się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO;
- zobowiązanie do pomocy administratorowi w wywiązaniu się z obowiązków określonychw art. 32–36 RODO;
- ustalenia dot. Postępowania z danymi po zakończeniu świadczenia usług związanychz przetwarzaniem (zależnie od decyzji administratora: usunięcie lub zwrot);
- umożliwienie administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji.

Wzór umowy powierzenia stanowi Załącznik nr 5. Zapisy umowy powierzenia mogą być włączone jako jeden z paragrafów umowy biznesowej lub mogą stanowić odrębną umowę, w której preambule przywoła się umowę biznesową.

Przed zawarciem umowy, w ramach której będzie dochodziło do przetwarzania danych osobowych, Administrator weryfikuje, czy potencjalny podmiot przetwarzający wdrożył niezbędne środki techniczne i organizacyjne, zapewniając spełnienie wymagań RODO i niezbędną ochronę praw osób, których dane dotyczą, w szczególności, czy zapewnia środki techniczne i organizacyjne gwarantującą ochronę danych zgodną z RODO.

Pracownik od spraw administracyjnych odnotowuje fakt zawarcia umowy powierzenia odpowiednio w rejestrze czynności przetwarzania danych lub w rejestrze kategorii przetwarzania.

7.3. Rejestrowanie czynności przetwarzania

W Spółce prowadzone są dwa osobne rejestry czynności przetwarzania, w zależności od tego, czy czynności te podejmowane są przez Spółkę jako Administratora czy przez Spółkę występującą w roli podmiotu przetwarzającego. Rejestry prowadzone są w formie elektronicznej. Wzór rejestrów zawarty jest w Załączniku nr 6.

Każdy z rejestrów otwiera strona tytułowa zawierająca nazwę i dane kontaktowe (adres, e-mail, nr telefonu) Administratora.

Rejestr czynności przetwarzania danych osobowych składa się z następujących pól:

- Nazwa czynności przetwarzania;
- Jednostka organizacyjna;
- Cel przetwarzania;
- Kategorie osób;
- Kategorie danych;
- Podstawa prawa;
- Źródło danych;
- Planowany termin usunięcia kategorii danych;
- Nazwa współadministratora i dane kontaktowe;
- Nazwa podmiotu przetwarzającego i dane kontaktowe;
- Kategorie odbiorców;
- Nazwa systemu lub oprogramowania;
- Ogólny opis techniczny i organizacyjny środków bezpieczeństwa;
- DPIA;
- Transfer do kraju trzeciego lub organizacji międzynarodowej.

Rejestr kategorii czynności przetwarzania danych osobowych składa się z następujących pól:

- Kategoria przetwarzania;
- Ogólny opis techniczny i organizacyjny środków bezpieczeństwa;
- Administrator;
- Nazwa i dane kontaktowe Administratora;
- Nazwa i dane kontaktowe współadministratora (gdy ma to zastosowanie);
- Nazwa i dane kontaktowe przedstawiciela administratora (gdy ma to zastosowanie);
- Czas trwania przetwarzania;
- Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane;
- Dokumentacja odpowiednich zabezpieczeń danych osobowych;
- Podprzetwarzajacy (nazwa i dane kontaktowe, kategorie podpowierzonych przetwarzań).

Na żądanie organu nadzorczego informacje o przetwarzaniu prowadzonym przez Spółkę (jako administratora lub jako podmiot przetwarzający) będą udostępniane organowi w sposób jednolity, czytelny i uproszczony, umożliwiający dokonanie ich szybkiego przeglądu i wstępnej weryfikacji.

Rejestry są prowadzone w formie osobnych plików *.xls*, za których aktualność i scalanie odpowiada Pracownik od spraw administracyjnych.

8. Procedura działania w przypadku stwierdzenia naruszenia ochrony danych osobowych

Naruszenie ochrony danych osobowych wynika z incydentu prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania danych osobowych lub z incydentu prowadzącego do nieuprawnionego ujawnienia danych lub nieuprawnionego dostępu do pomieszczeń lub zasobów teleinformatycznych, w których przetwarzane są dane.

Każdy, kto podejrzewa, że mogło dojść do wystąpienia incydentu jest zobowiązany do natychmiastowego kontaktu w tej sprawie z Prezesem Zarządu, która podejmuje następujące czynności:

1. Przeprowadzenie oceny skali incydentu i ustalenie, czy jego konsekwencją jest naruszenie ochrony danych osobowych (naruszenie praw i wolności osób fizycznych);
2. Zlecenie niezbędnych czynności w celu zminimalizowania skutków;
3. Jeśli zgłaszany incydent powoduje lub może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych – opracowanie i wysłanie zgłoszenie naruszenia ochrony danych osobowych organu nadzorczemu, zgodnie z treścią formularza udostępnionego na stronie Urzędu Ochrony Danych Osobowych. Zgłoszenie powinno zostać wysłane w ciągu 72 godzin od chwili stwierdzenia naruszenia, w przypadku przekroczenia tego terminu, należy wyjaśnić przyczyn opóźnienia.
4. Jeżeli naruszenie wpływa na osoby fizyczne w więcej niż jednym państwie członkowskim, zgłoszenie należy wysłać do właściwych organów nadzorczych w tych państwach
5. Jeśli zgłaszany incydent powoduje lub może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych – przygotowanie treści komunikatu oraz przekazanie go podmiotom danych w najbardziej efektywnej formie przekazu (korespondencja indywidualna, komunikat w prasie lub inna). Poszkodowanym podmiotom danych należy przekazać informacje dotyczące działań, jakie powinni podjąć, aby uchronić się przed konsekwencjami naruszenia ochrony danych osobowych. Wzór zawiadomienia osoby, której dane dotyczą stanowi Załącznik nr 7.
6. Wszelkie naruszenia i podjęte działania w celu ograniczenia ich skutków odnotowuje się w wewnętrznej ewidencji naruszeń ochrony danych osobowych, wg wzoru zawartego w Załączniku nr 8.

9. Definicje

Administrator - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;

Osoba zajmująca się obsługą informatyczną – osoba lub komórka organizacyjna zajmująca się obsługa informatyczną Spółki;

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

naruszenie ochrony danych osobowych - naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych,przechowywanych lub w inny sposób przetwarzanych;

ograniczenie przetwarzania - oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

organ nadzorczy – Urząd Ochrony Danych Osobowych;

osoba upoważniona – pracownik Administratora lub podmiotu przetwarzającego, który na podstawie pisemnego polecenia Administratora może przetwarzać dane osobowe;

Pracownik– osoba zatrudniona w Spółce PKLD Sp. z o.o. na umowę o pracę lub osoba fizyczna świadcząca usługi na rzecz Spółki na podstawie umowy cywilnoprawnej;

podmiot danych – osoba, której dane dotyczą;

podmiot przetwarzający - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

profilowanie - dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

przetwarzanie - operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, np.: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

pseudonimizacja - przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

zbiór danych - uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

zgoda osoby, której dane dotyczą - dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

Załącznik nr 1. Wzór upoważnienia do przetwarzania danych osobowych

……..
Miejscowość i data

Upoważnienie do przetwarzania danych osobowych

Spółka PKLD Sp. z o.o., będąca Administratorem danych osobowych upoważnia Pana/ Panią:

……
Imię i nazwisko

zatrudnioną/ego w ……

……
Nazwa i adres firmy, w której zatrudniona jest osoba upoważniana[2]

do przetwarzania danych osobowych i jednocześnie poleca przetwarzanie danych osobowych, zgodniez wymaganiami RODO, Ustawy o ochronie danych osobowych i Polityki ochrony danych osobowych w Spółce PKLD Sp. z o.o., w zakresie następujących czynności[3]:

- ……..
- ……..
- ……..

Upoważnienie do przetwarzania danych jest ważne przez okres świadczenia pracy/usług przez osobę upoważnioną lub do jego odwołania.

……..……
Podpis Prezesa Zarządu

Oświadczenie osoby upoważnionej

Oświadczam, że zapoznałam/-łem się z wymaganiami RODO i obowiązującej ustawy o ochronie danych osobowych; znam zasady przetwarzania i ochrony danych osobowych obowiązujące w Spółce PKLD Sp. z o.o.; niniejszym zobowiązuję się do ich stosowania. Zobowiązuję się do zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczania przez cały okres świadczenia pracy/usług na rzeczSpółki PKLD Sp. z o.o. oraz po zakończeniu przeze mnie świadczenia pracy/usług na rzecz Spółki. Jednocześnie przyjmuję do wiadomości, że za niedopełnienie obowiązków wynikających z niniejszego oświadczenia ponoszę odpowiedzialność administracyjną lub karną.

……..……
Czytelny podpis osoby składającej oświadczenie

[2]Jeśli osoba upoważniana jest pracownikiem Spółki PKLD– uzupełnić podając nazwę i adres Spółki. Jeżeli upoważnienie wydawane jest osobie, która ma uzyskać dostęp do danych administrowanych przez Spółkę na podstawie odrębnej umowy o świadczenie usług, należy wpisać dane podmiotu zatrudniającego tę osobę (podmiotu będącego stroną umowy, z której wynika konieczność przetwarzania danych).
[3]Wpisać wszystkie procesy ()wg rejestru czynności), w których dochodzi do przetwarzania danych przez osobę upoważnioną.

Załącznik nr 2. Wzór rejestru osób upoważnionych do przetwarzania danych osobowych

Imię i nazwisko osoby upoważnionej	Firma, w której pracuje osoba upoważniona	Data oświadczenia/ upoważnienia/	Data cofnięcia/ odwołania upoważnienia	Data aktualizacji 1	Data aktualizacji 2	Skany

Załącznik nr 3. Wzór rejestru zapytań i żądań podmiotów danych

Numer porządkowy żądania	
Data otrzymania żądania	
Imię i nazwisko podmiotu danych zgłaszającego żądanie	
Czy to pierwsze czy kolejne (które?) żądanie zgłaszającego podmiotu danych?	
Czego dotyczy żądanie (prawo dostępu, prawo ograniczenia danych, sprostowania, inne)	
Podjęte czynności (np. udostępniono kopie usuniecie danych)	
Nazwisko osoby, która wprowadziła dane do systemu i data dokonania zmiany – jeśli dotyczy	
Podmioty, które poinformowano o żądaniu usunięcia danych – jeśli dotyczy	
Uzasadnienie (jeśli nie było możliwe zrealizowanie prawa, np. dane przechowywane w związku z realizacją umowy)	
Data udzielenia odpowiedzi podmiotowi danych zgłaszającego żądanie	
Treść odpowiedzi (link do pliku)	
Uzasadnienie opóźnienia odpowiedzi – jeśli dotyczy	

Załącznik nr 4. Rejestr ujawnień danych odbiorcom danych

Lp.	Nazwa odbiorcy danych	Data ujawnienia	Podstawa ujawnienia danych	Osoby, których dane ujawniono

Załącznik nr 5. Wzór umowy powierzenia

Umowa powierzenia przetwarzania danych osobowych

zawarta dnia ……

pomiędzy:

PKLD Sp. z o.o. z siedzibą w Bielawie, ul. Wspólna 71 -05-520 Bielawa wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod numerem KRS..... ,
zwana dalej **„Administratorem danych”** lub **„Administratorem”,** reprezentowana przez:

……

oraz

……

……
zwany dalej **„Podmiotem przetwarzającym”**, reprezentowana przez:

……

(zwana dalej „Umową”)

Preambuła

Strony związane są umową zawartą dn……., której przedmiotem jest.....(dalej: Umowa Główna). W związku z realizacją Umowy Głównej zaistniała konieczność przetwarzania danych osobowych. Mając na celu zapewnienie przetwarzania danych w sposób zgodny z prawem, Strony zawierają niniejszą Umowę, określającą zasady przetwarzania i ochrony danych osobowych, o poniższej treści:

§ 1
Powierzenie przetwarzania danych osobowych

1. W trybie art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (zwanego dalej „RODO”) Administrator danych powierza Podmiotowi przetwarzającemu dane osobowe, do przetwarzania na zasadach i w celu określonym w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodniez niniejszą umową, RODO oraz z przepisami prawa krajowego o ochronie danych osobowych.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi RODO, w szczególności zapewnia bezpieczeństwo przetwarzania danych zgodnie z art. 32 RODO.

§2
Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie umowy dane… .....[4]
2. Kategorie osób, których dane będą przetwarzane przez Podmiot przetwarzający na mocy niniejszej umowy stanowią osoby ..... [5]
3. Podmiot przetwarzający będzie przetwarzał następujące kategorie danych ..... [6]

[4] Podać rodzaj danych np. dane zwykłe oraz dane szczególnych kategorii
[5] Podać kategorię osób, których dane dotyczą) np. pracowników administratora, klientów administratora itd.
[6] Wpisać np. imię i nazwisko, adresu zamieszkania, nr PESEL itd.

4. Powierzone przez Administratora danych dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu..... [7].

§3
Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych,do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych.
2. Podmiot przetwarzający zobowiązuje się po przetwarzania powierzonych danych w swojej siedzibie znajdującej się w……..... oraz… ..... [8]
3. Podmiot przetwarzający zobowiązuje się do dopuszczenia do przetwarzania danych osobowych wyłącznie osoby, którym nadał upoważnienie do przetwarzania danych osobowych oraz wydał pisemne polecenie przetwarzania danych w zakresie nieprzekraczającym uprawnień Podmiotu przetwarzającego, wynikających z niniejszej Umowy.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie tajemnicy przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej Umowy, zarównow trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
5. Podmiot przetwarzający po zakończeniu świadczenia usług związanychz przetwarzaniem usuwa/ zwraca[9] Administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, co potwierdza protokołem przekazanym Administratorowi danych niezwłocznie po dokonaniu tych czynności.
6. Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 RODO.
7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi – najpóźniej w ciągu 24 godzin od chwili stwierdzenia naruszenia

§4
Prawo kontroli

1. Administrator danych zgodnie z art. 28 ust. 3 pkt h) RODO ma prawo kontroli, przestrzegania przez Podmiot przetwarzający zasad przetwarzania danych na mocy niniejszej Umowy, a Podmiot przetwarzający zobowiązany jest umożliwić przeprowadzenie kontroli osobie wskazanej przez Administratora.
2. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum dwudniowym jego uprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora.
4. W przypadku kontroli prowadzonej przez organ nadzorczy, Podmiot przetwarzający niezwłocznie informuje o tym Administratora i umożliwia mu wzięcie udziału w kontroli.

§5
Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający nie będzie korzystał z dalszego powierzenia danych osobowych objętych niniejszą Umową, bez uprzedniej pisemnej zgody Administratora.
2. W przypadku dalszego powierzania przetwarzania danych, Podwykonawca winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzającyw niniejszej Umowie.
3. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za wszelkie szkody powstałe w wyniku działań lub zaniechań osób trzecich, którym powierzył wykonanie czynności na rzecz Administratora.

§6
Czas obowiązywania umowy

[7] Podać cel np. realizacji Umowy Głównej.
[8] Uzupełnić odpowiednio.
[9] Właściwe wybrać.

1. Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas *nieokreślony/określony od…….....do .....*[10].
2. Administrator ma prawo rozwiązania umowy w trybie natychmiastowym w przypadku stwierdzenia, że Podmiot przetwarzający nienależycie wywiązuje się z obowiązujących go przepisów prawa wzakresie przetwarzania danych osobowych oraz zobowiązań niniejszej umowy.

§7
Kary umowne

1. W przypadku stwierdzenia, że Podmiot przetwarzający nienależycie wywiązuje sięz obowiązujących go przepisów prawa w zakresie przetwarzania danych osobowych oraz zobowiązań niniejszej umowy Administrator ma prawo żądać od Podmiotu przetwarzającego zapłaty kary umownej w wysokości ..... , a Podmiot przetwarzający zobowiązuje się do zapłaty tej kary w terminie 14 dni od doręczenia mu wezwania do zapłaty, przelewem, na wskazany w wezwaniu numer rachunku bankowego.

§8
Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz RODO.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy Administratora.

_____	_____
Administrator danych	Podmiot przetwarzający

[10] Można wpisać, że czas obowiązywania umowy uzależniony jest od Umowy Głównej.

Załącznik nr 6. Wzory rejestrów czynności przetwarzania danych osobowych

Rejestr czynności przetwarzania

Administrator danych: PKLD Sp. z o.o. z siedzibą w Bielawie, ul. Wspólna 71 05-520 Bielawa,e-mail: rodo@jumpy.pl telefon: 692-711-580

LP.	Nazwa czynności przetwarzania	Cel przetwarzania	Kategorie osób	Kategorie danych	Podstawa prawna	Źródło danych	Planowany termin usunięcia kategorii danych *(jeżeli jest to możliwe)*	Nazwa współadministratora i dane kontaktowe *(jeśli dotyczy)*	Nazwa podmiotu przetwarzającego i dane kontakowe *(jeśli dotyczy)*	Kategorie odbiorców *(innych niż podmiot przetwarzający)*	Nazwa systemu lub oprogramowania	Ogólny opis technicznych i organizacyjnych srodków bezpieczeństwa zgodnie z art. 32 ust. 1	DPIA (jeśli tak, lokalizacja raportu)	Transfer	
														Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)	Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń
		Art.. 30 ust. 1 pkt b	Art.. 30 ust. 1 pkt c	Art.. 30 ust. 1 pkt c			Art.. 30 ust. 1 pkt f	Art.. 30 ust. 1 pkt a	Art.. 30 ust. 1 pkt d	Art.. 30 ust. 1 pkt d		Art.. 30 ust. 1 pkt g		Art. 30 ust. 1 pkt e	Art. 30 pkt e
1.															

Rejestr kategorii czynności przetwarzania

Administrator danych: PKLD Sp. z o.o. z siedzibą w Bielawie, ul. Wspólna 71 05-520 Bielawa,e-mail: rodo@jumpy.pl telefon: 692-711-580

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

Załącznik nr 7. Formularz zawiadomienia podmiotu danych o naruszeniu przetwarzania jego danych osobowych

Zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

PKLD Sp. z o.o. z siedzibą w Bielawie ul. Wspólna 71 -05-520 Bielawa, jako Administratordanych, zgodnie z art. 33 RODO[11] niniejszym zawiadamia Pana/Panią..... o wystąpieniu naruszenia danych osobowych, które polegało na[12]
……
……
……
……
Naruszenie, o którym mowa może skutkować[13]……..
……
……
……
……

W celu zaradzenia naruszeniu ochrony danych osobowych/ minimalizacji skutków naruszenia zastosowano/planuje się zastosowanie[14] następujących środków[15] ……..
……
……
……
……

Informacji w sprawie ww. naruszenia udzieli ……..… [imię i nazwisko] …….
Nr tel. …… adres e-mail……
W przypadku pytań, prosimy o kontakt.

[11] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
[12] Krótko opisać charakter naruszenia ochrony danych osobowych.
[13] Opisać możliwe konsekwencje naruszenia ochrony danych osobowych ze szczególnym uwzględnieniem skutków dla osoby, której dane dotyczą.
[14] Niepotrzebne skreślić.
[15] Opis zastosowanych środków.

Załącznik nr 8. Wzór wewnętrznej ewidencji naruszeń i incydentów w PKLD Sp. z o.o.

Numer naruszenia/incydentu	
Rodzaj incydentu	
Data i godzina wystąpienia incydentu	
Czy incydent zakwalifikowano jako naruszenie	Tak/Nie
Data i godzina stwierdzenia naruszenia	
Opis przyczyn i przebiegu incydentu	
Konsekwencje	
Działania naprawcze	
Miejsce incydentu – jeśli można określić	
Nazwa i dane kontaktowe podmiotu przetwarzającego - jeśli jest przyczyną incydentu	
Nośniki danych, których dotyczy incydent	
Kategoria i przybliżona liczba osób, których dane dotyczą	
Kategoria i przybliżona liczba wpisów, których dotyczy incydent	
Zagłoszenie organowi nadzorczemu	Tak/Nie
Data i godzina wysłania zgłoszenia	
Wyjaśnienie przyczyn opóźnienia zgłoszenia- jeśli dotyczy	
Link do treści zgłoszenia	
Wyjaśnienie powodów braku zgłoszenia – jeśli dotyczy	
Inne organy krajowe poinformowane o naruszeniu – jeśli dotyczy	
Zawiadomienie osoby, której dane dotyczą	Tak/Nie
Data wysłania zawiadomienia	
Sposób komunikacji	
Link do treści zawiadomienia	
Wyjaśnienie powodów braku zawiadomienia – jeśli dotyczy	
Ocena ryzyka naruszenia praw i wolności osób fizycznych	
Inne kwestie nieujęte powyżej	