Polityka prywatności

Poniższa Polityka prywatności ma na celu poinformowanie o sposobie wykorzystywania przez Śląski Regionalny Fundusz Poręczeniowy sp. z o. o. danych osobowych, względem których spełniane są wszystkie wymogi Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 UE z dnia 27 kwietnia 2016 r. (dalej jako: „RODO").

§ 1

POSTANOWIENIA OGÓLNE

1. Polityka została opracowana w celu zapewnienia zgodności procesu przetwarzania danych osobowych z obowiązującymi przepisami prawa, w szczególności z Rozporządzeniem 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), oraz ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. poz. 1000).
2. Celem Polityki bezpieczeństwa przetwarzania danych osobowych w Śląskim Regionalnym Funduszu Poręczeniowym, zwanym dalej „ŚRFP" zwanej dalej „Polityką" jest wskazanie podstaw dla właściwego wykonania obowiązków Administratora danych w zakresie bezpieczeństwa i prawidłowej ochrony przetwarzanych danych osobowych.
3. Polityka określa zasady przetwarzania danych osobowych oraz ich zabezpieczenia, jako zbiór reguł i zaleceń, regulujących sposób ich zarządzania, ochrony i przetwarzania.
4. Polityka zawiera zestaw informacji dotyczących szacowania procesów przetwarzania danych osobowych oraz obowiązujących zabezpieczeń technicznych i organizacyjnych, zapewniających właściwą ochronę przetwarzania danych osobowych.
5. Opracowaną Politykę stosuje się do danych osobowych:
    a. przetwarzanych w systemach informatycznych,
    b. przetwarzanych na nośnikach elektronicznych,
    c. przetwarzanych w sposób tradycyjny.

§ 2

DANE ADMINISTRATORA

Administratorem danych jest:

Śląski Regionalny Fundusz Poręczeniowy sp. z o. o.
40-203 Katowice, Al. Roździeńskiego 188,
NIP: 954-23-67-405, REGON: 277483759, KRS: 0000005627
Sąd Rejonowy Katowice-Wschód, Wydział VIII Gospodarczy Krajowego Rejestru Sądowego

Kontakt:

Osoba odpowiedzialna: Bartosz Zawiślok
Telefon: +48 32 785 85 85
E-mail: admin@rfp.pl

§ 3

CELE I PODSTAWY PRZETWARZANIA DANYCH

1. Dane osobowe mogą być przetwarzane na podstawie:
   a. niezbędności do wykonania umowy lub do podjęcia działań przed jej zawarciem
   b. w celu prowadzenia marketingu produktów i usług własnych
   c. w celu wykonywania umów wiążących z podmiotami współpracującymi i nadzorującymi
   d. dochodzenia roszczeń i wierzytelności wynikających z umów
2. Zakres przetwarzania danych:
   a. realizacji i wykonywania umów
   b. działania analityczne i statystyczne
   c. komunikacji
   d. przetwarzanie celem realizacji umów z podmiotami powiązanymi
3. Przekazujemy Państwa dane wyłącznie podmiotom umiejscowionym w ramach Europejskiego Obszaru Gospodarczego i przez to podlegającym surowym przepisom unijnym o ochronie danych, lub takim, które wiąże odpowiedni standard bezpieczeństwa. Przekazywanie danych do krajów trzecich nie jest aktualnie przez nas praktykowane lub planowane
4. Dane przechowywane są przez okres nie dłuższy, niż jest to niezbędne dla celów, w jakich następuje ich przetwarzanie, z zastrzeżeniem wyjątków przewidzianych w RODO.
5. ŚRFP informuje osobę, której dane dotyczą o podstawie przetwarzania jej danych osobowych. Realizacja obowiązku informacyjnego może polegać na umieszczeniu informacji w miejscu ogólnie dostępnym, w siedzibie ŚRFP albo stronie internetowej.

§ 4

OBOWIĄZKI ADMINISTRATORA DANYCH OSOBOWYCH

1. ADO zobowiązany jest do podjęcia wszelkich działań, których celem jest zapewnienie prawidłowej ochrony danych osobowych, w szczególności zapewnienie przetwarzania danych ze szczególną starannością realizując następujące zasady:
   a. przetwarzanie zgodnie z przepisami prawa,
   b. zbieranie danych dla określonych celów i nie poddawanie dalszemu przetwarzaniu niezgodnie z tymi celami,
   c. dane będą merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
   d. przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, jednak nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania,
   e. zabezpieczenie środkami technicznymi i organizacyjnymi, które zapewnią rozliczalność, poufność i integralność.
2. W ŚRFP stosuje się zabezpieczenie, którego celem jest zmniejszenie ryzyka poprzez obniżenie prawdopodobieństwa zrealizowania zagrożenia lub też minimalizacja strat związanych ze zrealizowanym zagrożeniem: program antywirusowy, anonimizacja, pseudonominizacja, procedury bezpieczeństwa.

§ 5

ZARZĄDZANIE OCHRONĄ DANYCH OSOBOWYCH

1. Celem właściwej realizacji zamierzeń a także skutecznej ochrony danych osobowych należy stosować następujące obowiązki:
    a. przeszkolić pracowników uprawnionych do przetwarzania danych osobowych w zakresie zasad bezpieczeństwa,
    b. przypisać użytkownikom określonych cech pozwalających na ich identyfikację w systemach informatycznych, dających możliwość dostępu do przetwarzania danych osobowych odpowiednio do zakresu upoważnienia,
    c. okresowo kontrolować użytkowników sposób postępowania przy przetwarzaniu
    d. w przypadku stwierdzonych nieprawidłowości podejmować stosowne działania celem ich wyeliminowania,
    e. na bieżąco wdrażać nowe rozwiązania organizacyjne i techniczne, które wzmocnią bezpieczeństwo przetwarzania danych osobowych.
2. W procesie nadzoru należy szczególnie uwzględniać zabezpieczenie w zakresie integralności, poufności oraz rozliczalności przetwarzania danych osobowych.
3. W procesie zarządzania należy stosować działania, które spowodują, że pracownicy, użytkownicy zewnętrzni będą:
    a. odpowiednio przygotowani i wprowadzeni do przetwarzania danych osobowych,
    b. zapoznają się z obowiązującymi procedurami i zasadami przetwarzania danych osobowych w ŚRFP
    c. na bieżąco informowani o wszelkich zmianach w procedurach.

§ 6

ODPOWIEDZIALNOŚĆ PRACOWNIKÓW I UZYTKOWNIKÓW SYSTEMU

1. W celu osiągnięcia i utrzymania wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych konieczne jest szczególne zaangażowanie ze strony każdego użytkownika w zakresie ochrony danych osobowych.
2. Użytkownicy zobowiązani do informowania o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe bezpośrednio do ADO.
3. Użytkownicy są zobowiązani do:
    a. postępowania zgodnie z Polityką,
    b. zachowania w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia,
    c. ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem.
4. Wykonywania niezbędnych działań i w procesie przetwarzania danych celem zapewnienia właściwej ich ochrony, w tym celu powinni:
    a. przestrzegać procedur związanych z otwieraniem i zamykaniem pomieszczeń, a także z wejściem do obszarów przetwarzania danych osobowych osób nieupoważnionych,
    b. informować Administratora o podejrzanych osobach poruszających się w obszarze przetwarzania danych osobowych,

c. użytkownicy powinni na podstawie dokonanej identyfikacji ewentualnych zagrożeń, przedkładać Administratorowi projekty i propozycje nowych rozwiązań, których celem jest zwiększenie poziomu bezpieczeństwa ochrony danych osobowych.

§ 7

ODPOWIEDZIALNOŚĆ ZA NARUSZENIE ZASAD OCHRONY DANYCH OSOBOWYCH

Rozporządzenie ogólne o ochronie danych osobowych a także Kodeks Karny określają odpowiedzialność pracownika w przypadku naruszenia ochrony danych osobowych.

§ 8

EWIDENCJA OSÓB UPOWAŻNIONYCH

1. Administrator prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych.
2. Ewidencja jest prowadzona na bieżąco.
3. Ewidencja osób upoważnionych do przetwarzania danych osobowych

§ 9

DOSTĘP, SPROSTOWANIE I USUNIĘCIE DANYCH OSOBOWYCH

1. Administrator danych osobowych na wniosek osoby, której dane dotyczą umożliwia jej dostęp do danych oraz udziela informacji w zakresie określonym w ogólnym rozporządzeniu o danych osobowych.
2. Administrator danych osobowych na żądanie osoby, której dane dotyczą dokonuje sprostowania danych osobowych lub ich uzupełnienia. Osoba jest zobowiązana do złożenia żądania w formie pisemnej.
3. Administrator danych osobowych po złożeniu wniosku przez osobę , której dane dotyczą ma obowiązek usunięcia jej danych osobowych w przypadku gdy:
    a. dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
    b. osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;
    c. osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania;
    d. dane osobowe były przetwarzane niezgodnie z prawem;
    e. dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator.

§ 10

ZASADY POSTĘPOWANIA W PRZYPADKU NARUSZENIA LUB PODEJRZENIA NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Użytkownicy są zobowiązani do szczególnej staranności przy przetwarzaniu danych osobowych.

2. Użytkownicy każdorazowo przed przystąpieniem do pracy są zobowiązani do dokonania oceny i oględzin miejsca pracy pod kątem, czy nie dokonano jakichkolwiek nieuprawnionych działań związanych z ochroną danych osobowych przez osoby nieuprawnione.
3. Sytuacje, na które należy zwrócić szczególną uwagę to:
    a. próba nieuprawnionego dostępu do pomieszczenia lub dostępu do danych osobowych,
    b. naruszenie lub próba naruszenia integralności, poufności lub rozliczalności danych i systemu,
    c. niezamierzona zmiana lub utrata danych zapisanych na nośnikach jako kopie zapasowe,
    d. próba nieuprawnionego logowania lub inny sygnał wskazujący na próbę lub działanie wskazujące na nielegalny dostęp do systemu,
    e. losowe zdarzenia, takie jak brak zasilania, pożar itp.,
    f. stwierdzenie braku sprzętu informatycznego, jego części lub nośników zewnętrznych zawierających dane osobowe (wydruki, pamięć zewnętrzna, płyty CD, dysk twardy, itp.).
4. W sytuacji, gdy użytkownicy. stwierdzą naruszenie lub próby naruszenia ochrony danych osobowych, wówczas są zobowiązani do niezwłocznego poinformowania o tym fakcie Administratora.
5. Przed poinformowaniem Administratora o naruszeniu lub próbie naruszenia ochrony danych osobowych, użytkownik jest zobowiązany do:
    a. wstrzymania pracy, a także wykonywania jakichkolwiek działań, które mogłyby utrudnić ocenę i analizę stwierdzonych działań związanych z naruszeniem ochrony danych osobowych,
    b. zabezpieczenia materiałów, dokumentów, aby uniemożliwić dostęp osobom nieuprawnionym i dalsza stratę,
    c. wykonywania wskazówek Administratora.
6. Administrator powinien:
    a. dokonać oceny sytuacji, szczególnie dokonać oględzin stanowiska pracy, pomieszczenia, stanu zabezpieczenia pomieszczenia, potencjalne skutki związane z naruszeniem ochrony danych osobowych,
    b. podjąć dalsze działania stosowne do potrzeb i zaistniałej sytuacji.
7. Administrator jest zobowiązany do sporządzenia raportu z naruszenia ochrony danych osobowych
8. Administrator jest zobowiązany w terminie 72 godzin po stwierdzeniu naruszenia, zgłosić takie naruszenie organowi nadzorczemu, chyba że jest mało prawdopodobne, by takie naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
9. Sytuacja związana z naruszeniem lub próbą naruszenia ochrony danych osobowych powinna być przedmiotem analizy i wniosków celem uniemożliwienia podobnych zdarzeń w przyszłości.