Polityka świadczenia usługi weryfikacji podpisu elektronicznego w trybie online

Wersja 5.1

Data wydania: 13.05.2020

MADKOM SA

Al. Zwycięstwa 96/98

81-451 Gdynia

Spis treści

1. Wstęp

Polityka świadczenia usługi weryfikacji podpisu elektronicznego w trybie online (zwana dalej Polityką) pozostając w zgodzie z wymaganiami *Ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej* określa rodzaj, zakres, rozwiązania techniczne i organizacyjne świadczonych usług niekwalifikowanych w zakresie weryfikacji podpisu elektronicznego oraz pieczęci elektronicznej w trybie online przez MADKOM SA. Działalność MADKOM SA w zakresie świadczonych usług opiera się na obowiązujących aktualnie na terenie Rzeczypospolitej Polskiej przepisach prawnych.

2. Definicje i pojęcia

Dostawca usług zaufania – podmiot wpisany do jawnego Rejestru Dostawców usług zaufania prowadzonego przez Ministra właściwego do spraw informatyzacji.

Elektroniczne poświadczenie weryfikacji (inaczej: EPW) – dokument zawierający kompletny wynik weryfikacji podpisu elektronicznego lub pieczęci elektronicznej zawierający datę i czas wygenerowania, oraz unikalny Identyfikator weryfikacji.

Polityka – niniejszy dokument o nazwie „Polityka świadczenia usługi weryfikacji podpisu elektronicznego w trybie online".

Świadczenie usług drogą elektroniczną – wykonanie usługi świadczonej bez jednoczesnej obecności stron (na odległość), poprzez przekaz danych na indywidualne żądanie Usługobiorcy, przesyłanej i otrzymywanej za pomocą urządzeń do elektronicznego przetwarzania, włącznie z kompresją cyfrową i przechowywania danych, która jest w całości nadawana, odbierana lub transmitowana za pomocą sieci telekomunikacyjnej w rozumieniu *ustawy z dnia 16 lipca 2004 r. – prawo telekomunikacyjne.*

Identyfikator weryfikacji – znacznik umożliwiający potwierdzenie prawdziwości EPW i pozwalający na odtworzenie wyniku weryfikacji.

Usługi – usługi Świadczone drogą elektroniczną zgodnie z niniejszą Polityką.

Usługobiorca / Użytkownik - podmiot, korzystający z Usług lub z którym zawarto umowę o świadczenie usług drogą elektroniczną.

Usługodawca – firma MADKOM SA.

3. Podstawy prawne świadczenia Usług

Świadczenie Usług odbywa się przy uwzględnieniu następujących regulacji wewnątrzwspólnotowych i krajowych:

- Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz. U. z 2013 r. poz. 1422 ze zm.),
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) Nr 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 (RODO),
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z dnia 23 lipca 2014r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesienie do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (EIDAS),
- Ustawa z dnia 5 września 2016r. o usługach zaufania i identyfikacji elektronicznej (t.j. Dz. U. z 2019r., poz. 162)
- Ustawa z dnia 10 maja 2018r. o ochronie danych osobowych (t.j. Dz. U. z 2019r., poz. 1781)

- Ustawa z dnia 17 lutego 2005r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2005 nr 64 poz. 565);
- Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (t.j. Dz.U. z 2018r., poz. 1954 z późn. zm.);
- Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2019 r., poz. 1429);

MADKOM SA jest Dostawcą usług zaufania i funkcjonuje zgodnie z obowiązującym na terenie Rzeczypospolitej Polskiej prawem na podstawie wpisu do rejestru niekwalifikowanych Dostawców usług zaufania prowadzonego przez Narodowe Centrum Certyfikacji, w zakresie weryfikacji statusu certyfikatu na pozycji nr 1, uzyskanego w dniu 16 maja 2017r.

4. Rodzaje i zakres świadczenia usług zaufania

Usługodawca świadczy następujące usługi zaufania

a) usługa weryfikacji podpisu elektronicznego,
b) usługa potwierdzenia autentyczności Elektronicznego poświadczenia weryfikacji

Usługi są świadczone przy wykorzystaniu serwisu internetowego i usług sieciowych. System spełnia wymagania tzw. Rozporządzenia w sprawie eIDAS i do weryfikacji podpisów wykorzystuje unijny system list zaufania (TSL).

a. Usługa weryfikacji podpisu elektronicznego

Usługa weryfikacji podpisu elektronicznego cechuje się właściwościami szczegółowo określonymi w tabeli poniżej.

Dostęp do usługi:	https://weryfikacjapodpisu.pl https://weryfikacjapodpisu.pl/en
Obsługiwane formaty podpisów i pieczęci:	XAdES – ETSI EN 319 132 PadES – ETSI EN 319 142 CadES – ETSI EN 319 122 AsiC – ETSI EN 319 162
Profile podpisu:	XadES: BASELINE-B, BASELINE-T, BASELINE-LT, BASELINE-LTA PadES: BASELINE-B, BASELINE-T, BASELINE-LT, BASELINE-LTA CadES: BASELINE-B, BASELINE-T, BASELINE-LT, BASELINE-LTA
Zaufane listy	TSL zgodnie ETSI TS 119612
Status certyfikatu online	CRL OCSP
Rozszerzenia profili	XadES: • Otaczający (enveloping) • Otoczony (enveloped) • Dołączony (detached) CadES: • Otaczający (enveloping) • Dołączony (detached) PadES: • Otoczony (enveloped)

	AsiC: • AsiCS:XAdES • AsiCE:XAdES
Weryfikacja znacznika czasu	Tak
Odtwarzanie ścieżki certyfikacji dla certyfikatów podpisujących	Tak
Odtwarzania ścieżki certyfikacji dla znaczników czasu	Tak
Formaty EPW	Plik w formacie JSON Plik w formacie PDF Plik w formacie HTML
Algorytmy funkcji skrótu	SHA-1, SHA-224, SHA-256, SHA-512
Algorytmy podpisu	RSA
Sprawdzenie integralności podpisanych danych	Tak
Wykrywanie ataku kolizyjnego SHA-1	Tak
Maksymalna liczba jednocześnie weryfikowanych plików	Brak ograniczenia
Status weryfikacji certyfikatu podpisującego	Pozytywny Warunkowo pozytywny Negatywny

Wynik weryfikacji podpisu i pieczęci elektronicznej jest zmienny w czasie ze względu na upływ ważności danych służących składaniu podpisów, pieczęci i znaczników czasu. Stąd dla celów dowodowych system generuje Elektroniczne poświadczenie weryfikacji, które użytkownik może przechowywać. EPW zawiera unikalny Identyfikator weryfikacji pozwalający użytkownikom zweryfikować treści wyniku weryfikacji z momentu weryfikacji.

UWAGA: Jeśli podpis elektroniczny lub pieczęć elektroniczna zawiera znacznik czasu to weryfikacja dokonywana jest na czas zawarty w znaczniku czasu, w przeciwnym wypadku – na bieżący moment.

b. Usługa potwierdzenia autentyczności Elektronicznego poświadczenia weryfikacji

Usługa umożliwia uzyskanie potwierdzenia autentyczności EPW, poprzez uzyskanie dostępu do pełnego wyniku weryfikacji dysponując wyłącznie unikalnym Identyfikatorem weryfikacji. Pozwala na odtworzenie wyniku weryfikacji z momentu weryfikacji podpisu i pieczęci, dla którego użytkownik dysponuje Identyfikatorem weryfikacji.

5. Wynik weryfikacji podpisu i pieczęci elektronicznej

W wyniku przeprowadzonej weryfikacji podpisu i pieczęci elektronicznej system prezentuje następujące dane dla każdego podpisu i każdej pieczęci odrębnie:

Dane podstawowe	
Nazwa pliku	Nazwa pliku, w którym w procesie weryfikacji został odnaleziony co najmniej 1 podpis elektroniczny (lub pieczęć)
Integralność	Wynik weryfikacji integralności podpisanych danych
Podpisujący	Dane zawarte w nazwie powszechnej certyfikatu podmiotu podpisującego lub identyfikator podmiotu posługującego się

	Profilem Zaufanym dla podpisów zaufanych (tylko PL) oraz nazwa podpisującego w przypadku podpisów osobistych (tylko PL).
Rodzaj uwierzytelnienia	Informacja o rodzaju podpisu elektronicznego, w przypadku podpisów zaufanych dodatkowo nazwa powszechna pieczęci elektronicznej
Deklarowany czas złożenia podpisu	Deklarowany czas podpisania/złożenia pieczęci, z urządzenia podpisującego, zawarty w treści podpisu elektronicznego wraz z informacją o czasie we właściwej strefie czasowej użytkownika weryfikującego
Dane szczegółowe	
Funkcja skrótu	Zastosowana w podpisie/pieczęci funkcja skrótu np. SHA-256, prezentowana w postaci tagu
Profil podpisu/pieczęci	Profil podpisu/pieczęci, patrz tabela w punkcie 4.a
Podpisujący	Dane zawarte w nazwie powszechnej certyfikatu podmiotu podpisującego lub identyfikator podmiotu posługującego się Profilem Zaufanym dla podpisów zaufanych (tylko PL) oraz nazwa podpisującego w przypadku podpisów osobistych (tylko PL).
Deklarowany czas złożenia podpisu	Deklarowany czas podpisania/złożenia pieczęci, z urządzenia podpisującego, zawarty w treści podpisu elektronicznego wraz z informacją o czasie we właściwej strefie czasowej użytkownika weryfikującego
Rodzaj uwierzytelnienia	Informacja o rodzaju podpisu elektronicznego, w przypadku podpisów zaufanych dodatkowo nazwa powszechna pieczęci elektronicznej
Podpisano dokument/plik	Informacja o podpisanym dokumencie, w tym nazwa pliku, nazwa pliku zewnętrznego (o ile został podpisany) oraz informacja o numerze podpisanej rewizji dla podpisu formacie PAdES
Powód	Szczegółowa informacja o powodach braku poprawnej weryfikacji
Podpis zaufany	O ile dotyczy to prezentowane są dane: Id konta Profilu Zaufanego, Imię, Nazwisko, PESEL (tylko PL).
Znacznik czasu	Czas wskazany w znaczniku czasu wraz z informacją o czasie we właściwej strefie czasowej użytkownika weryfikującego, rodzaj znacznika czasu, wystawca znacznika czasu oraz wynik weryfikacji znacznika
Certyfikat podpisującego	Dane zawarte w certyfikacie klucza publicznego, w tym: Nazwę powszechną, Organizację, Kraj, Serialnumber, Numer seryjny, Nazwa podmiotu wystawiającego, Informacja o zaufanych lub niezaufanych wystawcy (TSL), Status certyfikatu, Okres ważności certyfikatu, Informacja o wyniku weryfikacji statusu certyfikatu CRL i OCSP

Elementy podpisu	Lista referencji elementów objętych podpisem/pieczęcią, w tym identyfikatory i nazwy plików, wynik i weryfikacji skrótu/sygnatury oraz wartości certyfikatu
Pełna ścieżka certyfikacji	Jak w wierszu „Certyfikat podpisującego” dla wszystkich certyfikatów wyższego rzędu
Pełna ścieżka certyfikacji dla znacznika czasu	Jw. w stosunku do znacznika czasu.

Uwaga: Interpretacja wyniku weryfikacji elektronicznych podpisów, pieczęci i znaczników czasu należy tylko i wyłącznie do użytkownika

6. Przetwarzanie danych w tym danych osobowych

Usługi świadczone przez Usługodawcę zgodnie z niniejszą Polityką świadczone są na rzecz Użytkowników w oparciu o pozyskane od nich dane, które są przetwarzane w zasobach Usługodawcy.

Kwestia przetwarzania danych, w tym danych osobowych, na urządzeniach końcowych została uregulowana na stronie „Polityka prywatności oraz polityka plików cookies wykorzystywanych w serwisie weryfikacjapodpisu.pl” pod adresem https://weryfikacjapodpisu.pl/cookies.html.

Administratorem danych przetwarzanych w ramach świadczonych Usług jest MADKOM SA z siedzibą w Gdyni (81-451), Aleja Zwycięstwa 96/98, zarejestrowaną w Sądzie Rejonowym Gdańsk Północ, VIII Wydział Gospodarczy Krajowego Rejestru Sądowego. KRS: 0000394954 NIP: 586-227-27-56 REGON: 221508925, z którym można skontaktować się na wyżej podane dane adresowe lub poprzez adres e-mail: madkom@madkom.pl.

Administrator wyznaczył Inspektora Ochrony danych z którym można skontaktować się na dane adresowe Administratora lub poprzez email: iod@madkom.pl.

GROMADZENIE I PRZETWARZANIE DANYCH W RAMACH ŚWIADCZONYCH USŁUG – ZAKRES, CEL, PODSTAWA, CZAS.

Wszelkie dane, w tym dane osobowe wykorzystywane w ramach Usług, realizowane są zgodnie z niniejszą Polityką. Dane nie są w żaden wykorzystywane przez Usługodawcę w żadnymi innym celu niż realizowanie Usług.

Administrator przetwarza dane użytkowników usługi (logi serwera i pliki cookies, choć co prawda nie są to dane, dzięki którym MADKOM SA może samodzielnie wprost zidentyfikować konkretną osobę fizyczną) w tym także dane przekazywane za pośrednictwem formularza kontaktowego, przez użyciu którego można się z dostawcą usługi skontaktować (przekazywane są w ten sposób dane takie jak: imię, nazwisko, numer telefonu czy adres e-mail).

W zakresie realizacji Usług, Administrator przetwarza dane, w tym dane osobowe zawarte w plikach przesyłanych do zasobów Administratora przez Użytkowników serwisu, chcących skorzystać z Usług i są to dane zamieszczone w przekazanych plikach, celem weryfikacji podpisów i pieczęci elektronicznych w nich zapisanych. Zakres powierzonych do przetwarzania danych zależy tylko i wyłącznie od Użytkowników. Użytkownicy korzystający z usługi dostępnej ogólnie przesyłając pliki, które będą przetworzone w celu uzyskania wyniku weryfikacji robią to akceptując Politykę świadczenia usług oraz Politykę prywatności obowiązującą na stronie. Przetwarzane dokumenty w ramach usługi nie są gromadzone przez MADKOM SA, ale w ramach usługi są przetwarzane, i po zweryfikowaniu podpisu/ów niezwłocznie usuwane. Istnieje także możliwość korzystania z usług poprzez interfejs API

(application programming interface) – w takim przypadku świadczenie usługi odbywa się w oparciu o Umowę Powierzenia Przetwarzania Danych Osobowych.

Procesy przetwarzania danych odbywają się bez ingerencji ludzkiej, czyli na żadnym etapie realizacji usługi dane Usługobiorcy nie są przetwarzane przez człowieka. Dane wykorzystywane w procesach świadczenia usług są usuwane z zasobów Administratora niezwłocznie po zrealizowaniu usługi. W zasobach Administratora pozostają jednak wyniki uzyskane w ramach realizacji usługi weryfikacji podpisu elektronicznego, umożliwiające w późniejszym czasie zweryfikowanie autentyczności wystawionego przez system Elektronicznego poświadczenia weryfikacji, wśród których znajdują się publiczne dane z certyfikatu mogące zawierać dane osobowe (np. PESEL).

Pełny wynik weryfikacji zawierający wszystkie dane z certyfikatów podpisujących w ramach usługi weryfikacji autentyczności Elektronicznego Poświadczenia Weryfikacji przechowywany jest przez okres 20 lat, ponieważ dokument elektroniczny, który powstaje jako udokumentowanie czynności prawnej, jest podpisywany podpisem elektronicznym (analogicznie do dokumentu papierowego podpisanego piórem). Poświadczenie może być wykorzystywane w procesach dochodzenia roszczeń, w których pełny wynik weryfikacji może być niezbędny. Po tym czasie wynik weryfikacji będzie nadal przechowywany i dostępny w historii weryfikacji, lecz pozbawiony danych osobowych podpisującego (w tym imion, nazwisk, numerów zawierających PESEL), które zostaną przez nas usunięte. Nadal zapewni to możliwość potwierdzenia prawdziwości i pewności poświadczenia weryfikacji, gdyż zawierać będzie ono najistotniejszą informację, tj. status ważności podpisu i pozostałe dane dotyczące wyniku weryfikacji podpisu elektronicznego.

ODBIORCY DANYCH

Odbiorcami danych, w tym danych osobowych, którym Administrator może powierzać dane, będą dostawcy usług prawnych, informatycznych, w tym podmioty zajmujące się hostingiem (przechowywaniem) danych dla Administratora. Odbiorcami danych, którym Administrator może dane udostępniać są organy publiczne.

Gromadzone przez nas dane, w tym dane osobowe nie są przekazywane organizacjom międzynarodowym czy do państw trzecich. Dane osobowe mogą być przetwarzane przez inne podmioty zgodnie z prawem Unii lub prawem krajowym.

7. Zobowiązania i odpowiedzialność

a. Zobowiązania w zakresie świadczonych usług

Usługodawca gwarantuje, że Usługi są świadczona zgodnie z niniejszą Polityką. Ponadto w organizacji funkcjonują procedury operacyjne oraz procedury zarządzania bezpieczeństwem, które wykluczają jakąkolwiek możliwość manipulowania wynikiem weryfikacji. W tym celu Usługodawca posiada wdrożony i certyfikowany System Zarządzania Bezpieczeństwem Informacji zgodny z ISO/IEC 27001.

b. Odpowiedzialność i zobowiązania MADKOM SA

Usługodawca gwarantuje, że działalność oraz świadczone usługi są zgodne z prawem i w szczególności nie naruszają praw autorskich i licencyjnych stron trzecich oraz że zatrudnia pracowników posiadających wiedzę, kwalifikacje i doświadczenie odpowiednie do pełnienia funkcji związanych ze świadczonymi Usługami, w szczególności obejmujących dziedziny:

- automatycznego przetwarzania danych w sieciach i systemach teleinformatycznych,
- mechanizmów zabezpieczania sieci i systemów teleinformatycznych,

- sprzętu i oprogramowania stosowanego do elektronicznego przetwarzania danych.

Usługodawca zapewnia ochronę przetwarzanych danych osobowych zgodnie 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).*

Usługodawca nie ponosi odpowiedzialności za szkody i problemy w działaniu Usługi. MADKOM SA nie ponosi odpowiedzialności także z tytułu czasowego lub stałego zawieszenia dostępności Usług, a w szczególności szkody lub problemy wynikające z awarii łącza lub jego niewystarczającej przepustowości leżące po stronie odbiorcy usługi.

O ile z przepisów prawa powszechnie obowiązującego nie wynika odmiennie, w zakresie zobowiązań związanych z niniejszą Polityką wobec Użytkowników ograniczona jest do szkód wyrządzonych umyślnie lub z powodu zaniedbania.

Usługodawca nie odpowiada za szkody powstałe w wyniku korzystania z Usług w sytuacji, gdy Użytkownicy będą wcześniej poinformowani o ograniczeniach w świadczonych Usługach i ograniczenia te mogą być przez Użytkowników rozpoznane.

Usługodawca nie ponosi odpowiedzialności za szkody wynikające z nieprzestrzegania przez Użytkowników zasad określonych w niniejszej Polityce.

c. Rozstrzyganie sporów

W przypadku zgłaszania zażaleń czy też wystąpienia sytuacji spornych powstałych na tle korzystania z Usług, Usługodawca będzie dążył do wyjaśnienia i polubownego rozstrzygnięcia w oparciu o pisemne informacje.

Zgłaszając szkodę ciężar dowiedzenia zamiaru lub zaniedbania Usługodawcy spoczywa na Użytkowniku zgłaszającym szkodę.

W przypadku nie rozstrzygnięcia kwestii spornych w drodze mediacji jak też w sprawach nieuregulowanych w zapisami niniejszej Polityki, lub indywidualnymi umowami, mają zastosowanie przepisy prawa polskiego.

8. Opłaty

Usługi objęte niniejszą Polityką świadczone nieodpłatnie, za wyjątkiem indywidualnie zawieranych umów.

9. Rejestrowanie zdarzeń

W celu nadzoru nad sprawnym działaniem Usług oraz w celu rozliczania Użytkowników oraz pracowników usługodawcy z ich działań, w systemie rejestrowane są wszystkie te zdarzenia i działania, które mogą mieć istotny wpływ na bezpieczeństwo funkcjonowania systemu i świadczonych w nim Usług. Rejestr zdarzeń może być przeglądany tylko i wyłącznie przez upoważnionych pracowników Usługodawcy, a zapisy rejestru zdarzeń nie mogą być modyfikowane.

Wszelkie przesłane dokumenty do weryfikacji przez Użytkowników są usuwane natychmiast po przeprowadzeniu weryfikacji.

10. Zabezpieczenia komunikacji

Komunikacja pomiędzy komputerem użytkownika a serwerem usług, jest zaszyfrowana z użyciem protokołu SSL (Secure Socket Layer). Protokół SSL to rodzaj zabezpieczenia, polegający na kodowaniu danych przed ich wysłaniem z przeglądarki użytkownika i dekodowaniu po bezpiecznym dotarciu na serwer. Informacja wysyłana z serwera do klienta jest również kodowana, a po dotarciu do celu dekodowana. Protokół SSL szyfruje, uwierzytelnia i zapewnia integralność wiadomości.

11. Zakończenie działalności lub zaprzestanie świadczenia usług

W przypadku zaprzestania świadczenia usług opisanych w niniejszej Polityce, Usługodawca dołoży wszelkich starań, by ograniczyć szkody Użytkowników. W przypadku wystąpienia takiej sytuacji opublikowana zostanie z wymaganym wyprzedzeniem informacja o zakończeniu działalności, a klienci z którym będą w tym czasie zawarte umowy komercyjne zostaną powiadomieni zarówno za pośrednictwem uwierzytelnionej poczty elektronicznej jak i tradycyjnej w odpowiednim czasie (zgodnym z zapisami indywidualnej umowy).

12. Administrowanie Polityką

Dokument Polityki jest wersjonowany i każda kolejna wersja Polityki zaczyna obowiązywać z chwilą jej zatwierdzenia i opublikowania. Powodami wydania kolejnej wersji dokumentu mogą być uaktualnienia czy też błędy występujące w aktualnej wersji. Nowa wersja w trakcie opracowywania posiada status dokumentu roboczego i jest przygotowywana tylko i wyłącznie przez uprawnionych pracowników Usługodawcy. Dokument jest zatwierdzany przez Prezesa Zarządu spółki MADKOM SA.

13. Ochrona informacji

MADKOM SA gwarantuje, że wszystkie będące w jego posiadaniu informacje są gromadzone, przechowywane i przetwarzane zgodnie z obowiązującymi w tym zakresie przepisami prawa. Stosowanie najwyższych standardów bezpieczeństwa informacji potwierdza fakt posiadania przez MADKOM SA aktualnego Certyfikatu Bezpieczeństwa Informacji PN-ISO/IEC 27001.

14. Historia dokumentu

Data / wydanie	Opis zmiany
05.2017 / wyd.1	Nowe wydanie dokumentu
10.2017 / wyd.2	Aktualizacja – zmiana nazwy serwisu
01.2018 / wyd.3	Aktualizacja – zmiana nazwy serwisu
06.2019/ wyd. 3.2	Aktualizacja – korekta
19.09.2019/ wyd. 4.0	Aktualizacja polityki w zakresie świadczonych usług niekwalifikowanych
15.11.2019/ wyd.5.0	Aktualizacja polityki związana z aktualizacją serwisu
13.05.2020 / wyd. 5.1	Aktualizacja w zakresie doprecyzowania okresu przetwarzania danych osobowych