Federacje PIONIER.Id i eduGAIN a RODO

W ramach federacyjnego dostępu do usług zewnętrznych, w momencie uwierzytelnienia, następuje przekazanie do dostawcy usług pewnego zestawu atrybutów, które w większości należy uważać za dane osobowe. Naturalne są zatem obawy osób odpowiedzialnych za ochronę danych w instytucjach akademickich poświadczających tożsamość . Na tej stronie zebraliśmy informacje, które mogą pomóc w uspokojeniu tych obaw oraz stworzeniu własnych lokalnych regulacji.

Poniżej zebrano następujące informacje:

1. Jak działa logowanie federacyjne

Mechanizmy logowania federacyjnego PIONIER.Id i eduGAIN polegają na wykorzystaniu systemów informatycznych instytucji akademickich do potwierdzania uprawnień pracowników i studentów do korzystania z zewnętrznych usług internetowych. Działa to podobnie tak jak logowanie poprzez konto Google lub Facebook do innych stron, np. sklepów internetowych.

W procesie federacyjnego logowania uczelnia występuje jako tzw. dostawca tożsamości (DT lub Identity Provider, IdP), zaś właściciela danej strony internetowej określa się jako dostawcę usługi (DU lub Service Provider, SP). Użytkownik trafia na stronę dostawcy usługi i zamiast zakładać nowe konto, wskazuje z jakiej jest uczelni i zostaje przekierowany na jej stronę internetową w celu zalogowania się. Po zalogowaniu się przez użytkownika, system uczelni potwierdza jego tożsamość dostawcy usługi i przekazuje mu pakiet minimalnych danych niezbędnych do udostępnienia usługi użytkownikowi. Całość procesu odbywa się za wyraźną zgodą użytkownika.

Rozwiązanie powyższe jest szeroko wykorzystywane w środowisku akademickim, ponieważ umożliwiają współpracę setek, a nawet tysięcy dostawców tożsamości (w skrócie DT bądź IdP), w tym przypadku uczelni, oraz usługodawców (w skrócie DU bądź SP) bez potrzeby zawierania umów dwustronnych, co przy skali środowiska akademickiego byłoby po prostu niewykonalne. Jak dotąd formuła sprawdza się, ponieważ pomimo działania

globalnych mechanizmów federacyjnych od ponad 10 lat, nie odnotowano żadnych istotnych incydentów z nimi związanych.

2. Charakter przekazania danych w świetle RODO

Rozważając ryzyko związane z procesem przekazania danych należy brać pod uwagę charakter tych danych. Przekazywane są jedynie podstawowe dane ze sfery przynależności pracownika i studenta do środowiska akademickiego. Zakres potrzebnych danych może być różny dla różnych usług, ale katalog danych obejmuje tylko imię, nazwisko, e-mail, specyficzny dla usługi identyfikator pseudonimowy, identyfikator w usłudze (np. identyfikator POLON), status w instytucji (student, staff, employee, itp. - zamknięty słownik) i identyfikator ORCID.

Przekazanie danych w procesie pozyskania dostępu do danej usługi odbywa się na życzenie użytkownika, od jednego administratora danych osobowych, którym jest uczelnia jako tzw. dostawca tożsamości, do drugiego administratora danych osobowych, którym jest dostawca usług. Można to uznać za jedną z form spełnienia artykułu 20, ust.2 RODO, czyli prawa do przenoszenia danych.

Uczelnia przekazując te dane w procesie logowania federacyjnego, po ich przekazaniu, nie odpowiada za dalsze ich prawidłowe przetwarzanie przez dostawcę usług, który jest samodzielnym administratorem danych osobowych. Przekazane dane są administrowane w ramach tej usługi, zgodnie z przepisami, w tym z polityką prywatności. Ewentualne prawa użytkownika, w tym do zaprzestania przetwarzania jego danych w usłudze, muszą być realizowane przez dostawcę usługi.

Wyjątkiem od powyższych ogólnych zasad są sytuacje, gdy mechanizm logowania federacyjnego jest stosowany w powiązaniu z dodatkowymi umowami zawartymi między dostawcą tożsamości a dostawcą usług, w ramach których przewidziane zostały specyficzne procedury przetwarzania danych osobowych. Oczywiście dostawca tożsamości może też posiadać własne dodatkowe mechanizmy wsparcia użytkowników w kwestiach przetwarzania danych osobowych w usługach zewnętrznych (wszystkich bądź wybranych).

Oczywiście logowanie federacyjne PIONIER.Id, poprzez podłączenie do światowego systemu eduGAIN, wykracza poza granice Polski i Unii Europejskiej. Wydaje się jednak, że o ile użytkownikowi zostanie przedstawiona pełna i prawidłowa informacja, ostatecznie to do niego należy decyzja o przesłaniu danych osobowych.

3. Rola uczelni jako dostawcy tożsamości (DT/IdP) w prawidłowym przekazaniu danych

Prawidłowo skonfigurowany proces uwierzytelnienia powinien zawierać krok poprzedzający udostępnienie jakichkolwiek danych, w którym użytkownik jest informowany o tym komu i jakie dane zostaną udostępnione. Użytkownik powinien potwierdzić przyjęcie tej informacji, ew. odstąpić od uwierzytelnienia w usłudze, zatrzymując w ten sposób proces przekazania danych. Można zatem przyjąć, że udostępnienie danych następuje zawsze za wiedzą i de facto na życzenie użytkownika. W celu uproszczenia kolejnych logowań do usługi użytkownik powinien mieć możliwość zaznaczenia, że nie chce być każdorazowo informowany o udostępnieniu danych, chyba że zakres tych danych ulegnie zmianie.

Zalecaną praktyką jest przygotowanie lokalnej aplikacji pozwalającej na wyświetlenie wszystkich usług, do których dane są udostępniane w czasie logowania, w wyniku wcześniejszych zgód użytkownika oraz odwołanie konkretnych zgód. Należy jednak wyraźnie zaznaczyć, że odwołanie zgody na automatyczne udostępnianie po stronie uczelni nie oznacza usunięcia z usługi zewnętrznej danych przekazanych wcześniej. Po przekazaniu, dane są w dyspozycji usługodawcy jako administratora danych osobowych i to on jest zobowiązany do odpowiedniej realizacji praw użytkownika.

Uczelnia będąca dostawcą tożsamości jako członek Federacji ma możliwość potwierdzenia tożsamości usługi, do której loguje się użytkownik. Jeżeli usługa udostępnia link do swojej polityki prywatności, to ten link powinien być pokazany użytkownikowi w ramach ekranu informacyjnego. Na ekranie informacyjnym powinien być też link do lokalnego regulaminu korzystania z usług zewnętrznych i szerszych opisów dotyczących danych osobowych. IdP zapewnia bezpieczny kanał komunikacji z dostawcą usługi tak, by wszelkie przekazywane atrybuty były szyfrowane.

IdP posiada wiarygodne dane o swoich użytkownikach i gwarantuje, że dane przekazywane do usług są prawdziwe oraz przygotowane zgodnie ze specyfikacjami definiującymi konkretne atrybuty. Na przykład, jeżeli definicja atrybutu zakłada, że stosowane są w nim wyłącznie dane z zamkniętego słownika, to IdP taki słownik stosuje; ew., jeżeli specyfikacja atrybutu przewiduje, że jego wartość jest jednoznacznie powiązana z konkretną osobą fizyczną i nie może nigdy wystąpić w odniesieniu do innej osoby, to IdP jest zobowiązane do stosowania odpowiednich mechanizmów, które to zapewnią.

Niezależnie od faktu, że usługi powinny minimalizować oczekiwania odnośnie danych, IdP powinno zdefiniować globalną politykę określającą, jakie dane są potencjalnie akceptowalne do udostępnienia i ew. poszerzać taki zakres w

odniesieniu do konkretnych usług po przeprowadzeniu analizy zasadności i ocenie ryzyka.

4. Rola dostawcy usługi (DU/SP)

Zakres udostępnianych danych zależy od usługi. Usługa powinna ten zakres sygnalizować w jakiś sposób, typowo wskazując w metadanych listę wymaganych atrybutów albo sygnalizując to przy pomocy znacznika kwalifikującego usługę do określonej kategorii. Operatorzy federacji rejestrujących usługi powinni weryfikować listy oczekiwanych atrybutów pod kątem ich minimalizacji i maksymalnej ochrony prywatności. Federacje, które za pośrednictwem eduGAIN pobierają informacje o usługach zarejestrowanych przez inne federacji polegają na prawidłowości działania tych federacji. Należy przy tym mieć świadomość, że w eduGAIN zrzeszone są również federacje spoza obszaru EOG.

5. Rola Federacji w przekazaniu danych

Federacja PIONIER.Id nie jest pośrednikiem w przetwarzaniu danych osobowych. Wszelkie dane są przekazywane bezpośrednim kanałem między uczelnią (IdP) i usługą (SP). Ten kanał może być zbudowany "wirtualnie" z użyciem mechanizmów przeglądarki internetowej użytkownika, zawsze jednak pomija serwery Federacji. Podobnie, żadne dane nie przepływają przez serwery konfederacji eduGAIN.

Zasadniczą rolą Federacji jest dostarczane zestawu wiarygodnych danych, dzięki którym strony, czyli IdP i SP, mogą wzajemnie poświadczać autentyczność partnera w komunikacji oraz korzystać z szyfrowania w celu zabezpieczenia danych.

Federacja jest odpowiedzialna za przegotowanie zestawu odpowiednich metadanych i zabezpieczenie go kluczem, który jest znany członkom federacji oraz serwerom eduGAIN (w celu redystrybucji metadanych do innych stowarzyszonych federacji). Federacja dba o bezpieczeństwo procesu przetwarzania i podpisywania tylko zestawu metadanych.

6. Mechanizmy podnoszące poziom ochrony użytkownika

GEANT Data Protection Code of Conduct

Jest to zestaw wytycznych, opisujących zasady, którymi musi się kierować usługodawca, aby zapewnić maksymalny poziom ochrony danych osobowych. Usługodawcy, którzy dokonali analizy swoich procesów mogą zaznaczyć ten

fakt w swoich metadanych, publikując odpowiedni znacznik. Pomimo, że deklaracja przestrzegania zasad jest jednostronna, to z uwagi na fakt ustanowienia zasad zaufania pomiędzy usługodawcą, a jego macierzystą federacją, można zakładać, że deklaracja jest publikowana z dobrej wierze. Niezależnie, eduGAIN utrzymuje serwis weryfikacyjny, którego celem jest sprawdzanie, że do realizacji Code of Conduct nie wkradają się błędy, np. że strony opisujące politykę prywatności nie są niedostępne.

Jednym z założeń deklaracji Code of Conduct przez usługę jest potwierdzenie, że wszelkie pobierane dane są faktycznie niezbędne do prowadzenia danej usługi. W ślad za tym idzie oczekiwanie, że IdP będą skłonne akceptować takie deklaracje i udostępniać atrybuty zgodnie z listą publikowaną przez usługę, nawet jeżeli wykracza ona poza standard przyjęty przez IdP. Znacznik Code of Conduct mogą też publikować IdP sygnalizując w ten sposób automatyczną zgodę na publikowanie atrybutów do wszystkich usług deklarujących Code of Conduct.

REFEDS Research and Scholarship (R&S)

Jest to kolejne podejście do problemu ułatwienia podejmowania decyzji o udostępnianiu danych. W tym przypadku zakłada się, że znacznik R&S mogą publikować wyłącznie niekomercyjne usługi prowadzone przez podmioty naukowe. Takie usługi oczekują otrzymania standardowego zestawu danych na temat użytkownika obejmujących: trwały identyfikator użytkownika przydzielony na potrzeby danej usługi, imię i nazwisko, email, przynależność do grupy użytkowników (studenci, pracownicy itp.).

Macierzysta federacja IdP jest zobowiązana, aby przed uruchomieniem publikowania znacznika R&S potwierdzić uprawnienia usługi do jego posiadania.

IdP, które są gotowe, aby udostępniać wskazany zestaw danych wszystkim usługom deklarującym R&S mogą ten fakt ogłaszać publikując odpowiedni znacznik w metadanych.

eduGAIN prowadzi usługę pozwalającą administratorom IdP potwierdzenie, że ich IdP faktycznie wysyła odpowiedni zestaw atrybutów.