Wirtschaftsportalverbund

Ausnahmeregeln für die WKÖ B2B Federation

Für die WKÖ B2B Federation gelten die in diesem Dokument festgelegten Ausnahmen von den Bestimmungen des WPV-Rulebooks (appr. 4.7.2017, WPV Verein)

Präambel

Der Vorstand des Vereins „Wirtschaftsportalverbund – Verein zur Entwicklung und Organisation föderierter Identitätsmanagementsysteme“ (WPV) hat beschlossen, dass dem Regelwerk des WPV zusätzlich zum Rulebook in der aktuellen Fassung 1.17 die nachfolgenden Regeln hinzugefügt werden. Es handelt sich dabei nach § 15 des Rulebooks um Ausnahmeregeln von den Bestimmungen des Rulebooks, die ausschließlich für die WKÖ B2B Federation gelten, aufgrund von deren konkreten Anwendungsfällen und Teilnehmern gerechtfertigt erscheinen und keine Wirkung auf andere Federations haben. Die Schaffung solcher Ausnahmeregeln soll das Zustandekommen der WKÖ B2B Federation erleichtern und somit fördern.

1.1.1 Liste der Ausnahmen

1.1 Die Bestimmung über die Unvereinbarkeit von FO und IdP in Punkt 12.2.a des Rulebooks gilt nur insoweit, als FO und IdP zwei verschiedene Rechtssubjekte sein müssen.

1.2 SP dürfen zugleich die Rolle eines SB einnehmen. Die Bestimmung über die Unvereinbarkeit dieser beiden Rollen in Punkt 12.2.b des Rulebooks sowie die Bestimmung in Punkt 10.2.3 des Rulebooks, wonach der SB die Identität der Benutzer nicht kennen und nicht bestimmen darf, und die Bestimmung in Punkt 10.2.1 des Rulebooks, wonach der IdP nicht feststellen kann, um welchen SP es sich handelt, gelten somit nicht.

1.3 Punkt 2.4 des Rulebooks, wonach die Federation nach einer dreistufigen Architektur aufgebaut ist und sämtliche Transaktionen zwischen IdP und SP über einen SB laufen müssen, gilt nicht. Soweit die Rollen des SP und SB ein einem Rechtssubjekt vereint sind, ist die technische Funktionalität des SB nicht erforderlich.

1.4 Die Punkte 7.3.5.1 und 7.3.5.2 (Beschränkung der Beobachtbarkeit) des Rulebooks gelten nur insoweit sie trotz der eben genannten Ausnahmen umsetzbar sind. Insbesondere kann nicht verhindert werden, dass ein IdP einsehen kann, welche Services ein Benutzer verwendet. Er darf jedoch darüber keine Daten speichern, die über das für die Erfüllung seiner Pflichten und Aufgaben Notwendige hinausgehen.

1.5 Ein Audit der FO durch die FA (Punkt 5.3) ist derzeit nicht vorgesehen

1.6 Audits der IdP und SB (Punkt 5.4) erfolgen in Form einer internen Prüfung anhand der für sie anwendbaren Teile des Rulebooks (Self-Assessment). Deren Ergebnis ist dem FO zur Kenntnis zu bringen und hat auch eine Darlegung zu enthalten, wie die Bestimmungen des Datenschutzrechts eingehalten werden. Die Meldung eines positiven Ergebnisses ist Voraussetzung für deren Akkreditierung durch den FO gemäß Kapitel 4 des Rulebooks. Self-Assessments und Akkreditierung durch den FO sind alle 2 Jahre zu erneuern.

1.1.2 Aufhebung dieser Ausnahmen

Die Ausnahmeregeln gelten auf unbestimmte Zeit. Der Vorstand des WPV und der FO der Federation „B2B-Federation“ evaluieren gemeinsam einmal jährlich, ob alle oder einzelne Ausnahmen weitergelten oder aufgehoben werden sollen. Grundlage dieser Evaluierung ist die

Bewertung der konkreten Risiken, die durch den Weiterbestand einer Ausnahme für die Teilnehmer an der gegenständlichen Federation, am WPV sowie den betroffenen Personen (Principals) entstehen bzw. zu entstehen drohen. Dabei sind insbesondere geänderte rechtliche Bestimmungen, Veränderungen an der Struktur der Federation- bzw. WPV-Teilnehmer sowie allfällige Erkenntnisse aus dem konkreten Betrieb der Federation in die Beurteilung mit einzubeziehen.

Die Entscheidung über die Aufhebung der Ausnahmen trifft der Vorstand des WPV unter Berücksichtigung der Ergebnisse der Risikobetrachtung und den konkreten Risikoszenarien. In der Regel ist für den Entfall bzw. die Abänderung von Ausnahmen ein Übergangszeitraum von 24 Monaten vorgesehen. Soweit konkreter Schaden für die Teilnehmer des WPV oder für die betroffenen Personen (Gefahr in Verzug) droht, kann eine unverzügliche Aussetzung oder Aufhebung von Ausnahmen durch den Vorstand des WPV angeordnet werden.