AK E-Zustellung
15.9.2015

Arbeitspaket 5
Recht/Rulebook

Markus Knasmüller
knasmueller@bmd.at

Übersicht über Aufgaben

- EU- Verordnung (elektronische Identifizierung und Vertrauensdienste): 18.9.2015 Durchführungsbestimmungen, Sicherheitsniveaus
- Internationale Beobachtung
- Wirtschaftsportalverbund
- Erweiterungen Rulebook

WE MAKE BUSINESS EASY!

Estland

- Sehr fortschrittlich
- Digitales Land, fast überall freien Internetzugang
- Steuererklärung, Behördengänge, Handelsregister, Medizin (Patientenberichte, Rezepte), erfolgt per Internet
- Wahl von daheim per Computer oder Smartphone
- Grundlage: elektronische ID-Karte, 2002 eingeführt
- Besitzen 1,1 der 1,3 Mio Einwohner Estlands
- Chip mit 2.048-bit Verschlüsselung
- Ausweis, Reisedokument und SV-Karte
- Auch als Mobil-ID für Smartphone erhältlich
- Seit 1.12.2014 auch für nicht in Estland ansässige Personen erhältlich (kein Reisedokument)

WE MAKE BUSINESS EASY!

Estland

- Verbunden mit ID-Karte Mailadresse
- Portallösung um Dokumente sicher und signiert auszutauschen
- Privatwirtschaftliche Plattformen
- www.signwise.me
- Speichert Dokumente unveränderlich

- *The only thing you can´t do online ist get married or buy a house.*

WE MAKE BUSINESS EASY!

Wirtschaftsportalverbund

- Kooperationsbasis für verschiedene Dienstanbieter der Wirtschaft
- Elektronische Geschäftsprozesse sicher und effizient abwickeln
- Single Sign On für viele unterschiedliche Geschäftsprozesse
- Wurde beobachtet, Teilnahme am AK WPV 23.6.2015
- WPV ist meiner Meinung nach noch nicht wie erhofft fortgeschritten
- ABER: Rulebook in erster Version veröffentlicht
- Noch keine Use Cases
- Da wird sich noch einiges tun

WE MAKE BUSINESS EASY!

Überblick Rulebook WPV

- Definitionen, Begriffe
- Architektur des WPV
- Voraussetzungen für Teilnahme
- Rechten und Pflichten für die Teilnahme
- Regeln für Aufnahme, Betrieb und Beendigung
- Unvereinbarkeiten
- Gebühren und Leistungen
- Datensicherheitsvorgaben
- Etwaige Abweichungen vom Rulebook
- Gerichtszuständigkeit, anwendbares Recht

WE MAKE BUSINESS EASY!

Zustellkopf als IdP

- Allgemeine Sorgfaltspflicht
- Geheimhaltung
- Beschränkung der Verknüpfbarkeit
- Meldeverpflichtungen
- Protokollierung

WE MAKE BUSINESS EASY!

Allgemeine Sorgfaltspflicht

7.1 Allgemeine Sorgfaltspflicht

7.1.1 Jeder Teilnehmer hat unabhängig von den in diesem Rulebook festgelegten Pflichten die ihm aufgrund seiner Rolle zukommenden **Aufgaben nach dem Stand der Technik mit der Sorgfalt eines ordentlichen Unternehmers zu erfüllen**, die dafür notwendigen Kenntnisse zu besitzen (§ 347 UGB, § 1299 ABGB) und insbesondere angemessene Datensicherheits-maßnahmen zu ergreifen.

7.1.2 Jeder Teilnehmer hat **Personal und gegebenenfalls Unterauftragnehmer zu beschäftigen**, das bzw. die über das erforderliche Fachwissen, **die erforderliche Zuverlässigkeit**, die erforderliche Erfahrung und **die erforderlichen Qualifikationen** verfügt bzw. verfügen.

WE MAKE BUSINESS EASY!

Geheimhaltung

7.2.2 Geheimhaltung

7.2.2.1 Teilnehmer dürfen die von ihnen verarbeiteten personenbezogenen und transaktionsbezogenen Daten nicht an andere Teilnehmer oder an Dritte weitergeben, es sei denn, dies ist im Zuge der Durchführung einer Transaktion nach den Regeln dieses Rulebooks erforderlich oder es liegt eine gesetzliche Verpflichtung nach den Bestimmungen der Europäischen Union oder eines ihrer Mitgliedstaaten oder einer der unter 7.5.1 genannten Fälle vor.

7.2.2.2 Jeder Teilnehmer hat seine Mitarbeiter schriftlich über die gesetzlich und/oder nach diesem Rulebook bestehenden Geheimhaltungs-, Datenschutz- und Datensicherheitspflichten zu belehren.

7.2.3 Datenminimierung

Jeder Teilnehmer darf nur jene Daten einsehen und verarbeiten können, die er benötigt, um eine bestimmte Transaktion durchzuführen bzw. seine Aufgaben im WPV zu erfüllen.

WE MAKE BUSINESS EASY!

Beschränkung der Verknüpfbarkeit

7.2.4 Beschränkung der Verknüpfbarkeit

7.2.4.2 Darüber hinaus sollen auch andere personenbezogene Attribute nur im erforderlichen Umfang übermittelt werden und für eindeutige Kontaktadressen wie E-Mail möglichst eine pseudonymisierte Version verwendet werden.

Etwa bei Suche wird das Geburtsdatum zurückgegeben, entspricht wahrscheinlich nicht.

WE MAKE BUSINESS EASY!

Meldeverpflichtungen

7.2.6 Meldeverpflichtungen

Ungeachtet der Pflicht zur Meldung von Verstößen gemäß § 7.3.2 dieses Rulebooks und ungeachtet allfälliger gesetzlicher Meldepflichten hat jeder Teilnehmer Vorfälle der Kompromittierung von Sicherheitsmaßnahmen, unbefugte Zugriffe, unbefugte Manipulationen und Fehlfunktionen betreffend Systeme, die er zur Erbringung seiner diesem Rulebook unterliegenden Dienste betreibt, an die FA zu melden, unabhängig davon, ob durch das zu meldende Ereignis ein Schaden entstanden ist.

Begründung: Diese Meldepflicht bezieht sich insbesondere auf Hacker-Angriffe aber auch auf unbefugte Handlungen die von Mitarbeitern der Teilnehmer oder mit deren Wissen durchgeführt werden. Die FA muss über die Informationssicherheitslage im WPV im Bilde sein, um wenn nötig geeignete Maßnahmen, wie insbesondere Anpassung des Regelwerks treffen zu können.

WE MAKE BUSINESS EASY!

Protokollierung

9.3.1 Ein IdP muss Protokoll über jeden Vorgang der Authentifizierung (Login und Logout) und der Übertragung von Identitätsdaten an einen SB führen.

Begründung: Es wird bewusst der Begriff „Übertragung“ und nicht „Übermittlung“ verwendet, um die Auslegung auszuschließen, dass nur Übermittlungen im Sinne des Datenschutzgesetzes erfasst sind (auch wenn derzeit nur dies denkbar erscheint).

9.3.2 Jeder solche Protokolleintrag muss enthalten, welche Attribute – nicht jedoch Attributswerte – betreffend welchen Benutzer zu welchem Zeitpunkt an welchen SB übermittelt wurden.

9.3.3 Jeder solche Protokolleintrag ist mit einer eindeutigen Nummer zu versehen, die auch dem SB, der Empfänger der Datenübertragung ist, zu übermitteln ist.

Müsste wohl nur umgesetzt werden, keine Rulebook-Anpassung nötig

WE MAKE BUSINESS EASY!

Weitere Anregungen

- Kapitel 5 Audit (überlegenswert für den Einstieg eines Zustelldienstes, Konformitätserklärung)
- Weiterverwendung von Benutzerdaten wird ausgeschlossen
- Haftungen sind genauer geregelt
- Abschlusskapitel das anwendbares Recht und Gerichtsstand regelt

WE MAKE BUSINESS EASY!

Nächste Schritte

- WPV: engerer Kontakt, Rulebook-Vorschläge
- Andere Länder überarbeiten
- Durchführungserlässe bei EU-Verordnung 18.9.