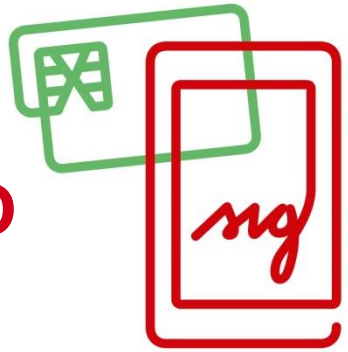
DIGITALES ÖSTERREICH

Die eIDAS-VO

und ihre legistische Begleitung in Ö (insbes. SVG, SVV)



E-Government Experts Group des Fachverbandes
Unternehmensberatung und Informationstechnologie

Wien, 27.4.2016

Peter.Kustor@bka.gv.at
Bundeskanzleramt
Abt. I/11

Der neue EU-Rechtsrahmen: die eIDAS-VO

28.8.2014 DE Amtsblatt der Europäischen Union L 257/73

VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 23. Juli 2014

über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

Eckpunkte eIDAS-VO

- Ein Rechtsakt für die beiden Themen eSignatur und eID
- Zusätzlich: weitere „Vertrauensdienste“
- Die SigRL (im SigG innerstaatlich umgesetzt) wird komplett ersetzt
- Typ des Rechtsakts: Verordnung
  - VO ist unmittelbar anzuwenden;
  - bestehende Umsetzungsvorschriften (SigG/ SigV etc.) sind zu bereinigen;
  - Umsetzungen und flankierende Regelungen sind aber notwendig
    (zB Verfahrensvorschriften, Zuständigkeiten, Ausnahmen, etc.)

„eIDAS-VO“: Überblick

- Kapitel I: Allg. Bestimmungen
- Kapitel II: **Elektronische Identifizierung**
- Kapitel III: **Vertrauensdienste**
- Kapitel IV: Elektronische Dokumente

- Kapitel V: Befugnisübertragungen und Durchführungsbestimmungen
- Kapitel VI: Schlussbestimmungen

- 4 Anhänge (Anforderungen an qual. Zertifikate/ Signaturerstellungseinheiten/ el. Siegel/ Website-Authentifizierung)

Definitionen zu eID

- "**Elektronische Identifizierung**" ist der Prozess der Verwendung von Personenidentifizierungsdaten in elektronischer Form, die eine natürliche oder juristische Person oder eine juristische Person vertretende natürliche Person eindeutig repräsentieren
- "**Personenidentifizierungsdaten**" sind ein Datensatz, der es ermöglicht, die Identität einer natürlichen oder juristischen Person oder einer eine juristische Person vertretenden natürlichen Person festzustellen
- "**Elektronisches Identifizierungsmittel**" ist eine materielle und/oder immaterielle Einheit, die Personenidentifizierungsdaten enthält und zur Authentifizierung bei Online-Diensten verwendet wird

eID (1/2)

- Keine Harmonisierung, keine „EU-eID“, keine zentrale Datenbank etc.
- Freiwillige Notifikation des eID-Systems durch den MS
- Voraussetzungen für die Notifikation
- 3 Sicherheitsniveaus:
  „Niedrig“ – „Substanziell“ – „Hoch“,
  mit Durchführungsrechtsakt definiert

eID (2/2)

- Verpflichtende gegenseitige Anerkennung der von den anderen MS notifizierten eIDs
- Sicherheitsniveau des eID ist gleich hoch oder höher als der verlangte Level („substanziell“ oder „hoch“)
- Anerkennung des Sicherheitsniveaus „niedrig“ auf freiwilliger Basis
- Für private Services auf freiwilliger Basis und unter den Konditionen des Ausstellers

Vertrauensdiensteanbieter (VDA) (1/2)

- Qualifizierte / Nicht-qualifizierte VDA
- Haftung: Beweislastumkehr bei qual. VDA
- Aufsicht über qual. VDA /
  reaktive (ex post) Maßnahmen bei nicht-qual. VDA („light touch approach“) – detaillierte Aufsichtsregelungen
- Sicherheitsanforderungen an VDA mit Notifikationspflichten bei Kompromittierungen
- Audit und Konformitätsprüfungen der qual. VDA
- Vorabgenehmigungsverfahren für qual. VDA und Vertrauensliste (TL) mit konstitutiver Wirkung
- „EU-Vertrauenssiegel“ für qual. Vertrauensdienste
- Anerkennung von qual. VDA aus Drittstaaten nur bei Abkommen mit EU

Vertrauensdiensteanbieter (VDA) (2/2)

- Anforderungen an qual. VDA betreffend
  - Identifikationsmechanismen bei Ausgabe von qual. Zertifikaten
  - Verlässlichkeit der Mitarbeiter
  - Finanzielle Ressourcen/ Versicherung
  - Informationspflichten
  - Sicherheitsanforderungen an die Systeme und Produkte
  - Dokumentationspflichten
  - Verzeichnis- und Widerrufsdienste etc.
  - „Notfall-(Einstellungs)pläne“ zur Sicherstellung der Kontinuität
- Allgemeine Bestimmungen zu Datenschutz, Accessibility, Strafbestimmungen

Vertrauensdienste (1/2)

- Elektronische Signatur – nat. Person
  - Rechtswirkungen wie bisher
  - Signaturformate in Anlehnung an Beschluss 2011/130/EU (XAdES, CAdES, PAdES, associated container)
  - SSCD – QSCD: verpflichtende Zertifizierung;
  - Berücksichtigung innovativer Möglichkeiten (server/remote signing; HSM etc.)

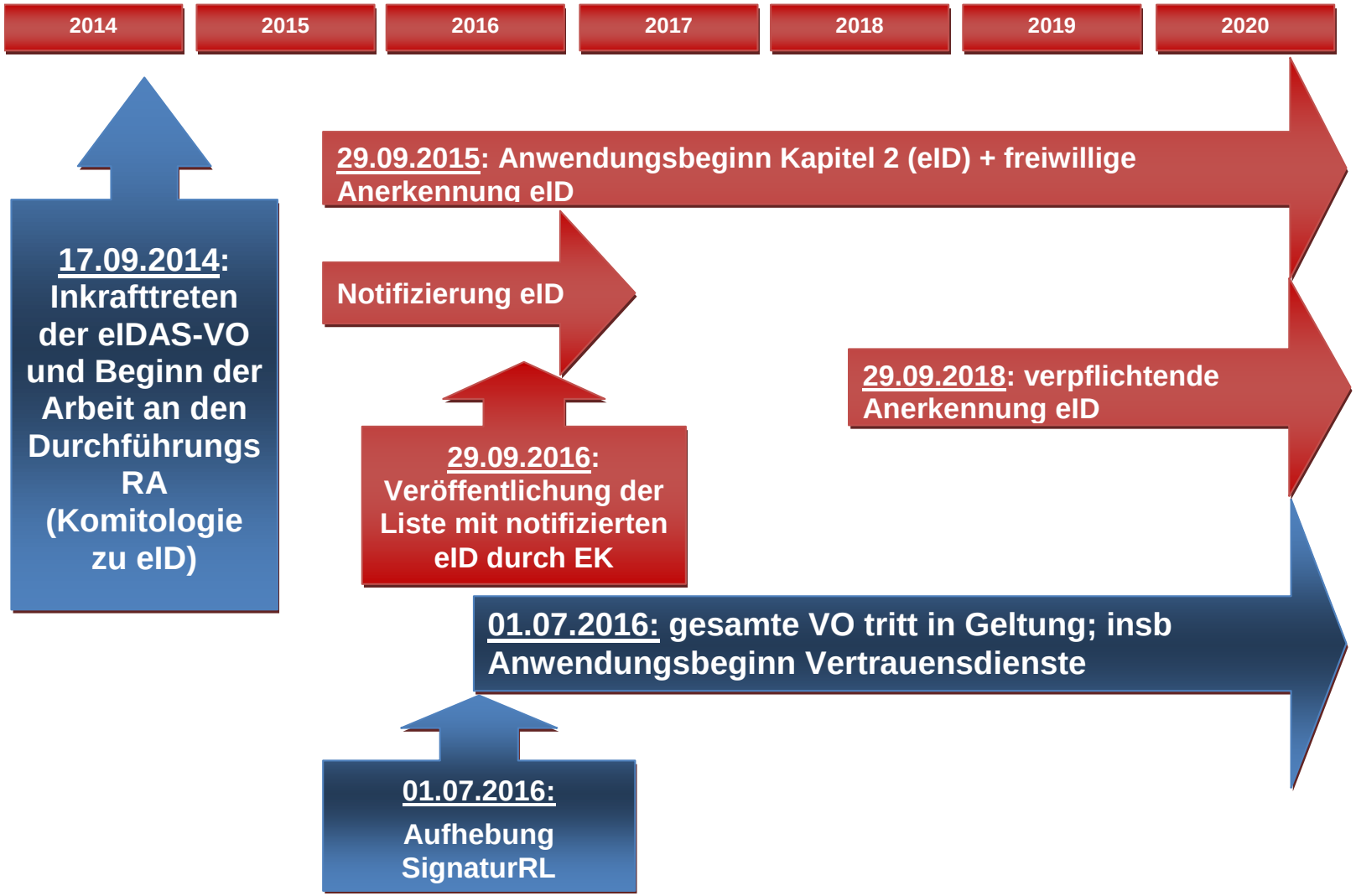
- Elektronische Siegel – jur. Person (weiter Begriff!)
  - Qual. Siegel: „Vermutung der Unversehrtheit der Daten und der Richtigkeit der Herkunftsangabe der Daten, mit denen das qualifizierte elektronische Siegel verbunden ist.“

Vertrauensdienste (2/2)

- Elektronische Bewahrungsdienste
- Elektronische Validierungsdienste
- Elektronische Zeitstempeldienste
- Elektronische Zustelldienste – „Dienste für die Zustellung elektronischer Einschreiben “
- Website Authentifizierung

Zu diesen fehlen derzeit noch weitgehend die relevanten internationalen Standards und damit die Durchführungsrechtsakte

Zeitplan eIDAS-VO



Legistische Umsetzung 1

- In der innerstaatlichen legistischen Durchführung werden nur jene Bereiche geregelt, in denen die unmittelbar anwendbare eIDAS-Verordnung den Mitgliedstaaten die Möglichkeit überlässt (oder die MS dazu verpflichtet), nationale Vorschriften zu erlassen.
- Dies betrifft im Bereich der Vertrauensdiensteanbieter insbes.: Aufsicht, Formvorschriften, Haftung und Sanktionen bei Nichteinhaltung der Vorgaben der Verordnung.
- Kern: Signaturen (auch Regelungen des aufzuhebenden SigG sind enthalten)

Legistische Umsetzung 2

- Erlassung eines Bundesgesetzes über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz – SVG)
- Aufhebung Signaturgesetz
- Novelle E-Government-Gesetz
- Legistische Anpassungen weiterer Bundesgesetze

- Begutachtungsfrist endete am 15.4.2016
- Geplantes Inkrafttreten: **1. Juli 2016**

Legistische Umsetzung 3

- Erlassung einer Verordnung über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdiensteverordnung – SVV)
- Aufhebung Signaturverordnung

- Begutachtungsfrist endet am 12.5.2016
- Geplantes Inkrafttreten: **1. Juli 2016**

SVG 1

- Beibehaltung Rechtswirkungen der Schriftlichkeit iSd § 886 ABGB einer qualifizierten el. Signatur
- Stärkung des Vertrauens in die Akzeptanz qualifiziert signierter Dokumente – Beseitigung der „versteckten“ Klauseln in AGBs (vgl. die Beschwerdefälle von Konsumenten bei Vertragskündigungen…)
- Pflichten von Signatoren und Siegelerstellern;
- Vorläufige Aussetzungsmöglichkeit;
- Ausstellung qualifizierter Zertifikate;

SVG 2

- Haftungsregelungen, Vertrauensinfrastruktur und Beendigungsplan für VDA;
- Festlegung der Aufsichtsstelle;
- Festlegung der Führung der Vertrauensliste bzw. eines Prüfservices;
- VO-Ermächtigung für die benannte Stelle;
- Sanktionen bei Verstößen.

Anpassungen E-GovG

- Beschränkt auf „unerlässliche“ Änderungen im Hinblick auf die eIDAS-VO (zB für Amtssignatur nun (auch) das fortg. el. Siegel)
- legistische Klarstellungen vor dem Hintergrund der Anwendungspraxis
- Verbesserungen in Bezug auf die Registernutzung bei Behördenverfahren (Entlastung für BürgerInnen und Unternehmen bei Vorlage von Nachweisen)

Anpassungen weiterer Gesetze

- Änderungen bei 22 weiteren Bundesgesetzen
- Keine inhaltliche Änderung sondern lediglich legistische Anpassung der Terminologie und der Verweisungen (statt SigG nun auf eIDAS-VO bzw. SVG…)

Was fehlt?

- Regelungen im Hinblick auf die Interoperabilität der österreichischen eID (Bürgerkarte – insbes. Handy-Signatur - in Bezug auf die eID-Funktion) und für die Anerkennung der ausl. eIDs in Ö sind NICHT Teil des vorliegenden Pakets
- Diese sollen zeitnahe in einem gesonderten legistischen Vorhaben vorgenommen werden

Danke

für Ihre Aufmerksamkeit!

Mag. Peter Kustor
Bundeskanzleramt
Abteilung I/11

Ballhausplatz 1
1014 Wien
i11@bka.gv.at
www.bka.gv.at