Datenschutzrechtliche Neuerungen für AMS Partnerinstitutionen

DI Robert Hörmann

7. Mai 2018

Inhalt

- Wozu das alles, in Zeiten von Facebook & Co?
- Was sind die neuen gesetzlichen Grundlagen?
- Was sind die wesentlichsten datenschutzbezogenen Verpflichtungen der Partnerinstitutionen des AMS?
- Was passiert, wenn Sie diese nicht einhalten?

Wozu das alles, in Zeiten von Facebook & Co?

Datenschutz wozu?

- **Schutz der personenbezogenen Daten ist ein Grundrecht**
  (Europäische Grundrechte-Charta)
- **Nutzen der Chancen und Minimieren der Risiken der Digitalisierung**
- **Haftung & Bußgelder**
- **Imageschaden**

Grundrecht auf Schutz der eigenen Daten

„Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.“

(Art. 8 Abs. 1 der Charta der Grundrechte der Europäischen Union)

„Diese VO schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten“

(Art. 1 Abs 2 Datenschutz-Grundverordnung – DSGVO)

„Jedermann hat Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten ...“

(Verfassungsbestimmung im § 1 Abs 1 DSG – entfällt mit Datenschutz-Deregulierungs-Gesetz 2018)

Was sind die neuen gesetzlichen Grundlagen?

Gesetzlichen Grundlagen

- **Datenschutz-Grundverordnung – DSGVO**
  Verordnung (EU) 2016/679 vom 27. April 2016 – in Geltung ab 25.5.2018

- **Datenschutzgesetz**
  idF des Datenschutz-Anpassungsgesetzes – BGBl. 120/2017 sowie dem Datenschutz-Deregulierungsgesetz 2018 – in Geltung ab 25.5.2018

- **Div. Materiengesetze** (z.B. AMSG, AMFG, EStG)
  - Materien-Datenschutz-Anpassungsgesetz

Grundsätze einer zulässigen Datenverarbeitung
Art. 5 DSGVO

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

Rechtmäßigkeit der Verarbeitung
Art. 6 DSGVO

- Einwilligung der betroffenen Person
- Erfüllung eines Vertrages
- Erfüllung einer **rechtlichen Verpflichtung**
- Schutz lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person
- **Wahrnehmung einer Aufgabe im öffentlichen Interesse** oder der öffentlichen Gewalt
- Wahrung berechtigter Interessen des Verantwortlichen oder Dritte, sofern Interesse oder Grundrechte der betroffenen Person nicht überwiegen.

Wichtige Begriffe I
Art. 4 DSGVO

- *Personenbezogene Daten*
  alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen
  - Name
  - Adresse
  - Ausbildung
  - Bild
  - IP-Adresse (kann, muss aber nicht)
  - etc.

Besondere Kategorien pb Daten

Art. 9 DSGVO

Die Verarbeitung personenbezogener Daten aus denen

- die rassische und ethnische Herkunft,
- die politische Meinung,
- die religiöse oder weltanschauliche Überzeugung,
- die Gewerkschaftszugehörigkeit

hervorgeht, sowie die Verarbeitung von

- genetischen Daten,
- biometrische Daten,
- Gesundheitsdaten oder
- Daten zum Sexualleben oder der sexuellen Orientierung

ist verboten oder **nur unter strengen Rahmenbedingungen** möglich.

Wichtige Begriffe II
Art. 4 DSGVO

- *Verantwortliche (derzeit: Auftraggeber)*
  die, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden

- *Auftragsverarbeiter (derzeit: Dienstleister)*
  die, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten

Auftragsverarbeiter des AMS

AMS kann zur Erbringung von arbeitsmarktpolitischen Dienstleistungen geeigneter Einrichtungen betrauen (§ 32 Abs. 3 AMSG).

Diese gelten als **Auftragsverarbeiter** des AMS – sie sind **„der verlängerte Arm des AMS“.**

Daten werden **für das AMS z.B.** erhoben, gespeichert, verändert, verknüpft, ev. offengelegt und schlussendlich gelöscht oder vernichtet.

Die Offenlegung der Daten zwischen AMS und Auftragsverarbeiter ist rechtlich **ohne Einwilligung** des Betroffenen möglich. Eine Einwilligung ist auch nicht einzuholen.

Was sind die wesentlichsten datenschutzbezogenen Verpflichtungen der Partnerinstitutionen es AMS?

Richtlinie „Allgemeine Grundsätze zur Abwicklung von Förderungs- und Werkverträgen“

Mit Unternehmen, die gemäß § 32 Abs. 3 AMSG mit der Erbringung von amp Dienstleistungen betraut werden, ist eine **Datenschutzvereinbarung** abzuschließen.

Derzeitiger Stand: Mit 1.1.2019 dürfen Verträge nur abgeschlossen werden, wenn die Vertragspartner zusätzlich einen **Nachweis über technische und organisatorische Maßnahmen** vorlegen können.

Bei fortlaufenden Geschäftsbeziehungen ist Nachweis regelmäßig zu erneuern. Die Umsetzung ist bei Vor-Ort-Kontrollen stichprobenartig durch das AMS zu überprüfen.

Datenschutzrechtliche Dokumente

- Datenschutzvereinbarung
- Datensicherheitserklärung inkl. der Nachweise
- Leitfaden zur Erstellung von Lebensläufen
- Informationsblatt für die betroffenen Personen

Löschungs- und Aufbewahrungs-pflichten der Träger

- Projekte, die **ab 1. 5. 2017** genehmigt wurden, haben die personenbezogenen Daten, die nicht abrechnungsrelevant sind, **nach genau 6 Monaten** zu löschen/vernichten. (davor genehmigte Projekte: 2 Jahre)

- Alle **abrechnungsrelevanten** Daten sind verpflichtend **7 (Werkvertrag) bzw. 10 Jahre (Förderungsvertrag)** ab Ende des Jahres in dem der Vertrag geendet hat, **aufzubewahren**.

- Nachrichten im **eAMS-Konto** werden **2 Jahre nach Erstellung** automatisch durch das AMS gelöscht.

Was passiert, wenn Sie die Verpflichtungen nicht einhalten?

Haftung für materieller sowie immaterieller Schaden

- Art. 82 Abs 1 DSGVO sowie § 29 Abs 1 DSG: Verantwortlicher und Auftragsverarbeiter haften nach außen gesamtschuldnerisch.

- Art. 82 Abs. 2 DSGVO: Auftragsverarbeiter haftet, wenn
  - er seinen auferlegten Pflichten nicht nachgekommen ist oder
  - unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat.

- Art. 28 Abs 4 DSGVO: Haftung des ersten Auftragsverarbeiters auch für Sub-Auftragsverarbeiter

Bußgelder
(Art. 83 DSGVO und § 30 DSG)

- Hält sich ein Auftragsverarbeiter nicht an die Weisungen des AMS, wird er selbst Verantwortlicher, mit allen Rechtsfolgen. (Art. 28 Abs. 10 DSGVO)

- Bei rechtswidriger Datenverarbeitung treffen ihn die Bußgeld-Sanktionen
  (bis zu 20 Mio. EUR oder bis zu 4 % des weltweiten Jahresumsatzes, es gilt das jeweils höhere)

- § 11 Datenschutz-Deregulierungs-Gesetz 2018 – bei erstmaligen Verstößen insb. Verwarnen.

Nichteinhaltung der Datenschutzvereinbarung und des Datensicherheitskonzepts

- Verstöße gegen die vereinbarten Verpflichtungen sind ein Indiz, dass keine ausreichenden Garantien im Sinne des Art. 28 Abs. 1 DSGVO vorliegen.

- Werden Bedenken nicht ausgeräumt, ist keine weitere Beauftragung möglich!

Herzlichen Dank für Ihre Aufmerksamkeit!

Für Fragen und Anregungen:

robert.hoermann@ams.at