avita solutions

massgeschneiderte Softwarebegeisterung.

EU-DSGVO Herausforderungen für IT Lösungen

ProIT 28.9.2017

Themen

- Ziel
- Firma Vorstellung
- Übersicht EU DSGVO
- Einwilligung
- Betroffenen Rechte
- Pflichten des Unternehmens
- Tipps
- Das Gute an der EU-DSGVO
- Q&A

Ziel

- Aufzeigen der Anforderungen, welche durch Datenverarbeitungs-Lösungen für die Umsetzung der EU-DSGVO abgedeckt werden müssen.

Wer sind wir?

aviita establishment

- Sitz in Balzers, Liechtenstein
- Gründung 2008
- Inhaber: Viktor Frick
- 11 Mitarbeiter

Was macht uns aus?

- Entwicklung von massgeschneiderten Softwarelösungen
- Auf Basis eines eigenen, modernen Frameworks
- Made in Liechtenstein
- Entwicklung, Beratung, Einführung und Support erfolgt durch eigene Mitarbeiter

Referenzen

Argus Sicherheitsdienst AG, Eschen

- Kernapplikation für Alarmverwaltung, Revierdienst, Werkschutz, Intervention, Rechnungsstellung

Stiftung Fürst von Liechtenstein, Vaduz

- Schlossverwaltung und CRM

First Advisory Group, Vaduz

- Kernapplikation für CRM, ERP, Transaktionsprüfung, FATCA, AIA und Dokumentenverwaltung

Schweizerischen Ärztekrankenkasse, St. Gallen

- Kernapplikation für CRM, ERP, Prämienabrechnung und Taggeldverwaltung

avita solutions

massgeschneiderte Softwarebegeisterung.

EU-DSGVO Übersicht

Übersicht EU-DSGVO

Einwilligung

- Einwilligung des Betroffenen
- Datenbearbeitung nur dem Zweck angemessen
- Beschränkung auf Daten welche Notwendig sind

Betroffenen Rechte

- Auskunftspflicht
- Recht auf Vergessen
- Datenportabilität
- Datenweitergabe
- Widerspruch

Pflichten des Unternehmens

- Privacy by Design
- Privacy by Default
- Verzeichnis der Verarbeitungstätigkeiten
- Meldepflicht Aufsichtsbehörden

Was sind personenbezogene Daten

Als personenbezogene Daten werden Informationen bezeichnet, die über in der EU ansässige Personen gehalten werden und bei ihrem Bekanntwerden diese Personen in irgend einer Weise schädigen könnten

- Sozialversicherungs- und Kreditkartendaten
- persönliche Finanzdaten
- Arbeitszeugnisse
- Behandlungsunterlagen, Diagnosen
- biometrische Daten
- persönliche Interessen, Vorlieben
- Handy Nr von VIP / PEP

Einwilligung

Personen bezogene Daten dürfen nur gespeichert und verarbeitet werden:

- nach Einwilligung des Betroffenen
- wenn die Person Vertragspartner ist und die Daten für die Erfüllung des Vertrags notwendig sind
- wenn die Daten für die Erfüllung einer rechtlichen Verpflichtung notwendig sind (Sorgfaltspflichten)
- Zur Geltendmachung von Rechtsansprüchen

Anforderungen an IT

- A Zeitpunkt und Art der Einwilligung muss für jeden Betroffenen gespeichert sein.

avita solutions

massgeschneiderte Softwarebegeisterung.

Betroffenen Rechte

Betroffenen Rechte

Auskunft	• Information • Herausgabe • Art. 15
Löschung	• Recht auf Vergessen werden • Art.17
Berichtigung	• Berichtigung • Ergänzung • Art. 16
Einschränkung	• Sperren • Art. 18
Übertragbarkeit	• Herausgabe • Automatische Übermittlung • Art. 20
Widerspruch	• Allgemein • Direktwerbung • Art. 21

Auskunft

Betroffener darf Auskunft einfordern über

- Zweck der Datenverarbeitung
- Welche Daten werden gespeichert
- Wie lange werden die Daten gespeichert
- Wer hat Zugriff auf welche Daten
- Herkunft der Daten

Die geforderte Auskunft muss innerhalb eines Monats erteilt werden.

Auskunft

Anforderungen an IT

- Verzeichnis aller Daten-Speicherorte und Aufbewahrungsfristen
- Möglichst wenige Datenspeicherorte für personenbezogene Daten
  -> zentrale CRM / HRM
- Möglichst wenige Daten in Papierform
  -> elektronisches Archiv / DMS für alle Dokumente und eMails
- Keine Daten in persönlichen eMails-Posteingängen
- Keine Dokumente in Benutzer-Ordnern

Auskunft

Anforderungen an IT

Vorteil der digitalen Datenspeicherung!

Datenauskunft Firma XY

Stand: 15.6.2018

Nat. Person

Name	**Frick**	Vorname	**Viktor**
Ledigname		Vorname 2	**Walter**
Geburtsdatum	**25.6.1968**	Geburtsort	**Vaduz**
eMail	viktor.frick@aviita.li	Telefon Geschäft	**+423 / 388 12 12**
Handy privat		Handy Geschäft	**+423 / 787 12 12**

Identifikationen

AHV-Nr	**243.123.123**	**Schweiz**
PEID	**123333**	**Liechtenstein**

Beziehungen

Geschäftsführer	**aviita est.**	**Balzers, Liechtentein**	**1.4.2014**
Präsident	**ratatäsch Guggenmusik**	**Schaan, Liechtenstein**	**25.4.2015**
Vorstandsmitglied	**Verein XY**	**Buchs SG, Schweiz**	**1.1.2005**

Mandate / Aufträge

Buchhaltung	**aviita est.**	**Balzers, Liechtentein**	1.1.2008 -
Gründung	**aviita est.**		30.6.2007 – 15.2.2008

Dossier / Akten mit Bezug zu den Mandaten

Buchhaltung	**Ordner**	**1.1.2014-31.12.2015**	**Archiv1**
Buchhaltung	**Ordner**	**1.1.2016-31.12.2016**	**Archiv1**
Buchhaltung	**Ordner**	**1.1.2017-**	**Schrank XY**
Gründungmappe	**Mappe**		**Diskretarchiv**

eMails / Dokumente

eMail Eingang	78
eMail Ausgang	25
Verträge	3
Korrespondenz	12
Bankdokumente	9

Vergessen werden

Daten müssen gelöscht oder anonymisiert werden bei

- Widerruf der Einwilligung
- Erlöschen der Notwendigkeit der Datenspeicherung
- Beendigung der Kundenverhältnisses und Ablauf der gesetzlichen Aufbewahrungsfristen (z.B. 10 Jahre

Vergessen werden

Anforderungen an IT

- Anforderungen der rechtlichen Aufbewahrungsfristen berücksichtigen
- Definierter Datenlöschungsprozess notwendig
- Verzeichnis aller Daten
- Führen eines Verzeichnisses über den Widerruf der Datenverarbeitung
- Löschungsprozess unterstützt in den CRM/ERP/DMS Systemen
- Aufzeichnung von technischen Daten wie ChangeLogs müssen auch gelöscht werden

Vergessen werden

Anforderungen an IT

- Ermittlung und Speicherung der Aufbewahrungsdauer bei der Aufnahme von personenbezogenen Daten auf jedem Datensatz bzw. jedem Dokument
- Versehen von Akten/Dossier mit geplantem Vernichtungsdatum
- Eintragung der Aufbewahrungsfristen für alle Daten bei Beendigung der Kundenbeziehung (definierter Beendigungsprozess)

Datenportabilität

- Aushändigen der Daten an Betroffenen in maschinenlesbarer Form
- Weiterleitung der Daten an bestimmte Stellen nach Weisung des Betroffenen
- Für bestimmte Branchen API Definitionen für elektronische Weitergabe
  - Krankenversicherungen
  - Telekom Anbieter
  - Banken

Anforderungen an IT

- Einfache Abfrage der gespeicherten Daten
- Export in strukturierter Form
- Unterstützung der jeweiligen API

avita solutions

massgeschneiderte Softwarebegeisterung.

Pflichten des Unternehmens

Pflichten des Unternehmens

Privacy by Design	• Datenschutz durch technische und organisatorische Massnahmen
Privacy by Default	• Datenschutzfreundliche Voreinstellungen
Gewährleistung Schutzniveau	• Gewährleistung angemessenes Schutzniveau • Gemäss aktueller Technik
Verstärkte Dokumentation	
Verzeichnis der Datenverarbeitungstätigkeiten	
Datenschutz Folgenabschätzung	
Meldepflicht	• Innert 72h bei Aufsichtsbehörde

Privacy by Design

Datenschutz durch geeignete technische und organisatorische Massnahmen

Anforderungen an IT

- Berechtigungsmodell: Jeder Anwender sieht nur die Daten, die er für seine Arbeit benötigt (Rollenkonzept)
- Zugriffsrechte auf Datensatzebene
  Meine Kunden: nur Benutzer X sieht die SteuerNr, andere Benutzer sehen nur den Namen und die Adresse
- Verschlüsselung von personenbezogenen Daten mit hohem Risiko

Privacy by Design

Anforderungen an IT

- Protokollierung der Datenveränderungen
  Wer hat das Geburtsdatum des Kunden erfasst
- Protokollierung der Datenzugriffe
  Wer hat bei Kunde XY die SozialversicherungsNr angesehen
- Anonymisierung von Daten z.B. in BigData Anwendungen
- Regelmässige Prüfung der Privacy Einhaltung

Privacy by Default

Datenschutzfreundliche Voreinstellungen

Anforderungen an IT

- Erfassung von ausschliesslich notwendigen Daten (Datensparsamkeit)
- Regelmässiges Löschen von nicht mehr benötigten Daten
- Automatische Berechtigungsvergabe durch CRM/ERP System. Dabei gilt: so wenig Rechte wie möglich für Benutzer

Meldepflicht

Meldung eines Verstosses innerhalb von 72 Stunden nach Erkennung bei Aufsichtsbehörde

Anforderungen an IT

- Protokollierung der Zugriffe auf Personen bezogene Daten
- Laufende Überwachung der Datenzugriffe

Tipps

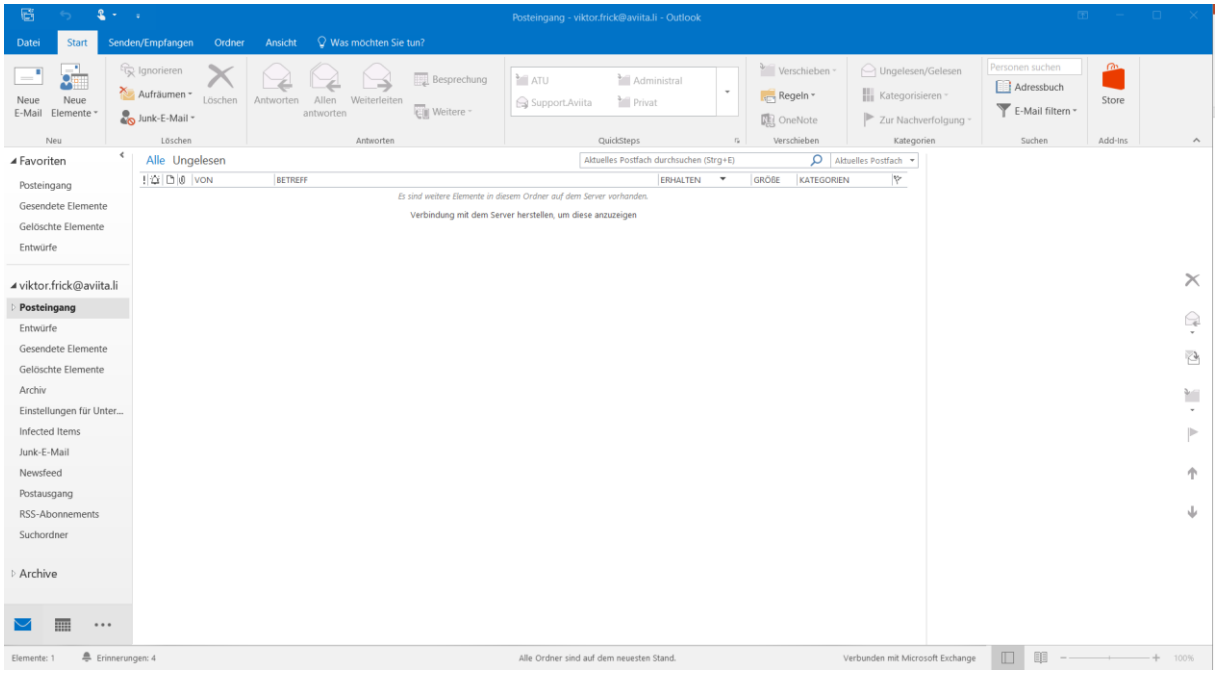
- Alle personenbezogenen Daten wenn möglich in **einem** zentralen System (CRM / HRM) speichern und verarbeiten
- Akten, Dokumente und eMails elektronisch und **zentral** speichern in Archivsystem / DMS
- Keine Datenfriedhöfe (z.B. Excel)
  Adressen für Weihnachtskarten, Kundenanlässe, Werbemail Verteiler
- Sensitive Daten wie Personaldossier und Bewerbungsdossier zentral speichern (verschlüsselt) und wenn es nicht mehr benötigt wird, löschen

Tipps

- Nur anonymisierte Daten dürfen einer Software-Entwicklungsfirma zur Verfügung gestellt werden
- Testsysteme sollten regelmässig aktualisert oder anonymisiert werden
- Genaue Backup-Strategie definieren
- Daten Restore
  Nur Daten zurückladen die benötigt werden,
  oder nicht benötigte Restore Daten sofort wieder löschen,
  oder Daten aus widerruf gemäss Verzeichnis wieder löschen

Tipps

- Keine Dokumente auf Desktop / persönlichen Ordnern
- Exchange ist kein Archivsystem
- So sollte ein Posteingang aussehen



Das Gute an der EU-DSGVO

- Optimieren der Datenspeicherorte (Aufräumen)
- Verbesserung des Berechtigungsmodells
- Dokumentation der wichtigsten Unternehmensprozesse
- Reduzierung der Datenmenge

Noch Fragen ?