Lehmann Computer

DSGVO und DSG-Revision

Technische Umsetzung

Roger Lehmann, Lehmann Computer
Betrieblicher Datenschutzverantwortlicher

Agenda

- Datensicherheit / Datenschutz
- Was sind personenbezogene Daten / Arten
- TOMs (Technische und Organisatorische Massnahmen)
- Privacy-by-design, Privacy-by-default
- Verzeichnis von Verarbeitungstätigkeiten
- Datenschutz-Folgeabschätzung (DS-FA)
- Datenschutzbeauftragter / Vertreter in der EU
- Anpassungen auf der Homepage / Datenschutzerklärung

Lehmann Computer

Datensicherheit / Datenschutz

Die Ähnlichkeit der beiden Wörter könnte dazu verleiten, anzunehmen, es handle sich um Synonyme. Aber das Gegenteil ist der Fall!

Datensicherheit / Toms

Als Datensicherheit oder globaler noch Informationssicherheit bezeichnet man die Eigenschaften von IT-Systemen die die Vertraulichkeit, Verfügbarkeit und die Integrität der Informationen sicherstellen.

Datenschutz

Der Datenschutz bezieht sich nicht auf die vorhanden Daten sondern auf deren Ursprung. Es geht im wesentlichen um das Recht, selbst zu bestimmen wie mit den eigenen, persönlichen Daten umgegangen werden soll.

Fazit

Die Datensicherheit kann den Datenschutz zwar unterstützen indem personenbezogene Daten vor unberechtigtem Zugriff geschützt werden. Aber gerade Backups und Speicherung von Daten in Could-Speichern bergen für den Datenschutz ein enormes Risiko und damit Missbrauchspotetial.

Was sind personenbezogene Daten / Arten / Datenschutz

Personenbezogene Daten
sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen und dadurch Rückschlüsse auf diese Person oder ihre Persönlichkeit erlauben, zum Beispiel:

- Name und Geburtsdatum
- Kontaktdaten wie Postanschrift, E-Mail-Adresse, Telefonnummer
- Körperliche Merkmale, z.B. Grösse, Gewicht, Haarfarbe
- Beziehungen wie Verwandtschaft, Freundschaften oder der Arbeitgeber
- Bankverbindungen

Besonders schützenswerte personenbezogene Daten.
Die Verarbeitung dieser Daten unterliegt strengen Voraussetzungen. Darunter fallen zum Beispiel:

- ethnische Herkunft
- politische, religiöse und weltanschauliche Meinungen
- Gesundheitsdaten
- Daten zum Sexualleben
- biometrische Daten zur eindeutigen Identifizierung einer Person

TOMs (Technische und Organisatorische Massnahmen)

Zutrittskontrolle	Verhindern, dass Unbefugte Zutritt zu den Datenverarbeitungsanlagen haben.	Alarmanlage
Zugangskontrolle	Verhindern, dass Unbefugte Datenverarbeitungsanlagen nutzen können.	Passwortverfahren
Zugriffskontrolle	Gewährleisten, dass nur Berechtigte auf Daten zugreifen können und diese nicht unbefugt gelesen, verändert, kopiert oder entfernt werden können.	Berechtigungskonzepte
Weitergabekontrolle	Gewährleisten, dass Daten bei der elektronischen Übertragung/Transport nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	Verschlüsselung / VPN
Eingabekontrolle	Gewährleisten, dass nachträglich überprüft werden kann, ob und wer Daten verändert oder entfernt hat.	Protokollierung / Protokollauswertungssysteme
Auftragskontrolle	Gewährleisten, dass Daten, die im Auftrag verarbeitet werden, nur entsprechend den Anweisungen des Auftraggebers verarbeitet werden können.	Vertragsgestaltung bei ADV
Verfügbarkeitskontrolle	Gewährleisten, dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	Datensicherung /Backup / Firewall / Virenschutz
Trennungsgebot	Gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden	Mandanten / Trennung der Systeme

Typische Schwachstellen? / Datensicherheit

- Papierentsorgung & Abfalleimer
- USB-Sticks, Speicherkarten & Datenträger
- Mobile Endgeräte
- Kommunikation & eMail
- Datensicherung & Datensicherheit
- Rechtesystem

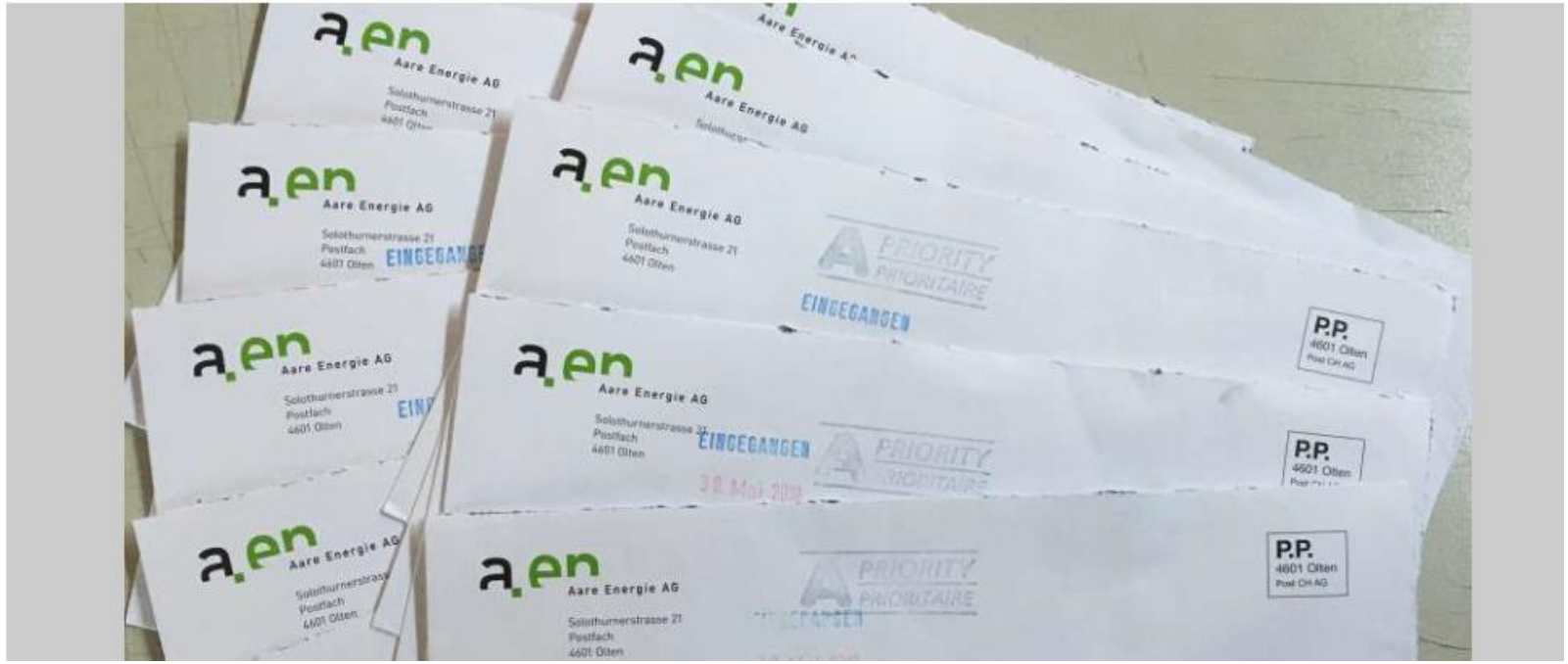
Lehmann Computer

Blick vom 24.06.2018

Oltner Stromfirma entsorgt Mahnungen im Altpapier

Kurzschluss bei Aare Energie

OLTEN SO - Da staunt eine BLICK-Leserin nicht schlecht: In einem Gemeinschafts-Container einer riesigen Überbauung in Olten findet sie etliche Briefe der Aare Energie AG. Und merkt: Es sind äusserst heikle Kundendaten, die die Firma im Altpapier entsorgt hat.



Fehler / Datensicherheit

- Zugang zu Betriebsräumen
- Aussagen am Telefon
- Offener Umgang mit vertraulichen Unterlagen
- Datenschutz nur im Büro (vs. Reise, HomeOffice, …)
- Schwache Passwörter & Weitergabe
- Schlecht gewartete Hard- und Software

Angriffszenarien / Problematik Big-Data

- Intern (Social Hacking, Datenklau, ... > 90% aller Fälle!)
  Trojaner, Phishing, Viren, Erpressung
  Hardware-Fehler

- Kombinationen von Attributen wie Geburtsdatum, Geschlecht und Postleitzahl: US-Wissenschaftler stellten fest, dass sich vier Fünftel der amerikanischen Bevölkerung allein mittels dieser drei Merkmale nachträglich identifizieren lassen.

- Aus durchschnittlich 68 Facebook-Likes eines Users kann vorhergesagt werden, welche Hautfarbe er hat (95-prozentige Treffsicherheit), ob er homosexuell ist (88-prozentige Wahrscheinlichkeit), und ob er Demokrat oder Republikaner ist (85 Prozent). 70 Likes reichen, um die Menschenkenntnis eines Freundes zu überbieten, 150 um die der Eltern, mit 300 Likes kann die Maschine das Verhalten einer Person eindeutiger vorhersagen als deren Partner

Privacy-by-Design

„Privacy by Design“ bedeutet „Datenschutz durch Technik“

und soll sicherstellen, dass Datenschutz und Privatsphäre schon in der Entwicklung von Technik beachtet werden. Technik ist dann so angelegt, dass die Privatsphäre von NutzerInnen geschützt wird und, dass AnwenderInnen Kontrolle über die eigenen Informationen haben.

Privacy-by-Default

Privacy by Default heißt übersetzt „Datenschutz durch datenschutzfreundliche Voreinstellungen“

und bedeutet, dass die Werkeinstellungen datenschutzfreundlich auszugestalten sind. Nach dem Grundgedanken sollen insbesondere die Nutzer geschützt werden.

Wo stehe ich im Moment?

Ist-Stand kennen!

- Datenschutzanalyse
- Datenschutzkette prüfen: wo sind und wer arbeitet mit meinen Daten?

Wohin will ich?

- Datenschutzniveau definieren:
- Was will ich umsetzen?
- Wieviel benötige ich / will ich mir leisten?
- Welches Risiko bin ich bereit einzugehen?
- Betriebswirtschaftliche Betrachtung?
- Soll-Konzept erarbeiten
- Bedarf Datenschutzbeauftragter feststellen

Was sollte ich unbedingt tun?

Dokumente prüfen!

- Impressum
- Datenschutzhinweise
- Datenschutzerklärungen
- AGB
- Mitarbeiterverträge
- Datenschutzordner
- ...

Lehmann Computer

Was sollte ich unbedingt tun?

Technik prüfen! TOMS

- IT, EDV
- Externe Zugänge, VPN, Verschlüsselungen
- CRM, Dokumentenmanagement, Buchhaltung, HR
- Kommunikation: Telefon, eMail, Messenger
- Büro- und Ablauforganisation
- Papier: Druck & Entsorgung
- ...

Lehmann Computer

OK, ist mir aber alles zu viel und zu teuer ...

Risikomanagement

- Betriebswirtschaftlichen Nutzen erkennen
- Große Risiken vermeiden
- Kleine Risiken akzeptieren

Unternehmerrisiko

User Experience

Pflichten des Managements nach DSGVO

- Datenschutzleitlinien erstellen
- Datenschutz-Management-System installieren
- Technische und organisatorische Maßnahmen ergreifen
- Privacy-by-design, Privacy-by-default
- Zusammenarbeit mit Aufsichtsbehörden
- Meldeverfahren installieren
- Mitarbeiter schulen
- Regelmäßige Bewertung und Überprüfung der Maßnahmen
- Dokumentation

Lehmann Computer

Weitere Herausforderungen

Gegenüber Aufsichtsbehörden

- Haben wir einen Überblick über sämtliche Datenquellen?
- Wie hoch ist das Risiko-Level pro Datenquelle?
- Können wir nachweisen, wo personenbezogene Daten gespeichert sind?
- Können wir nachweisen, dass wir die notwendigen Prozesse etabliert haben?
- Haben wir Tools für die Dokumentation und die Protokollierung im Einsatz?

Interne Herausforderungen

- Was sind personenbezogene Daten?
- Wie erkennen wir personenbezogene Daten?
- Kontrollieren wir Zugriffsrechte?
- Protokollieren wir Nutzeraktivitäten für jeden Datenbestand?
- Inwiefern erschweren Duplizierung und schlechte Datenqualität das „Löschen und Vergessen”?

Verzeichnis von Verarbeitungstätigkeiten

Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen.

Dieses Verzeichnis enthält sämtliche folgenden Angaben:
- den Namen und die Kontaktdaten des Verantwortlichen
- die Zwecke der Verarbeitung
- eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenb. Daten

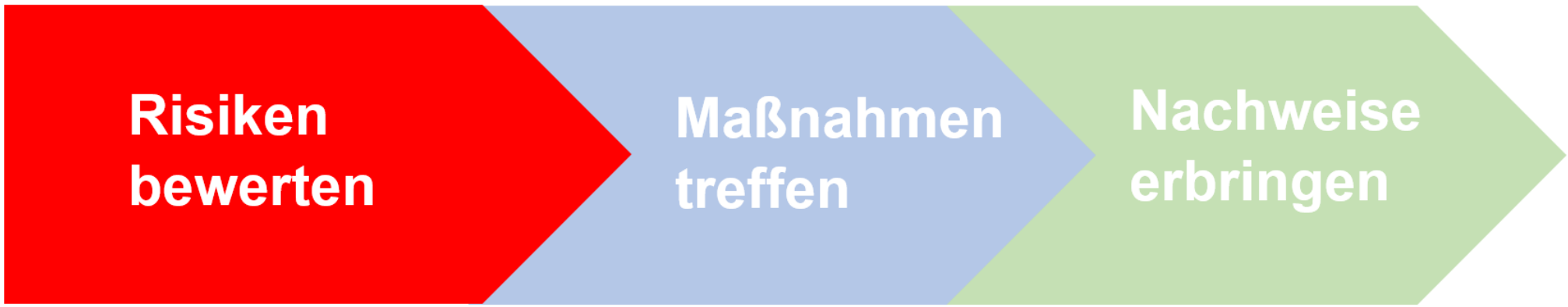
Lehmann Computer

Datenschutz Risiko- Folgeabschätzung

Auswirkungen aus Sicht der Betroffenen	Maximal	mittel	mittel	hoch	hoch
	Wesentlich	mittel	mittel	mittel	hoch
	Eingeschränkt	gering	mittel	mittel	mittel
	Vernachlässigbar	gering	gering	mittel	mittel
		Vernachlässigbar	Eingeschränkt	Wesentlich	Maximal
		Eintrittswahrscheinlichkeit			

Lehmann Computer

Lfd. Nr.	Datenfluss	Schadensschwere	Eintrittswahrscheinlichkeit	Rechte und Freiheiten	Art, Umfang, Zweck	Risikobewertung (insgesamt)
1	Erstkontakt	mittel, da weder unbedeutende noch besonders sensible Daten erhoben werden	hoch, weil in den vergangenen Jahren vermehrt Angriffe auf Unternehmen derselben Branche verübt worden (Quelle: www.xyz.de)	mittel, da weder untergeordnete noch besondere Rechte beeinträchtigt sind	hoch, da besonders viele Daten betroffen sind	gering: 0 mittel: 2 hoch: 2 **Gesamt: hoch**
2	Rückmeldung	gering, da nur die Kontaktdaten verarbeitet werden	hoch, da gerade bei Rückantworten in den vergangenen Jahren vermehrt Angriffe auf Unternehmen derselben Branche verübt worden (Quelle: www.xyz.de)	gering, da die für diesen Prozessschritt erforderlichen Daten keine besonderen Freiheiten tangieren	mittel, da zwar viele Betroffene, aber nur wenige Daten betroffen sind	gering: 2 mittel: 1 hoch: 1 **Gesamt: mittel**



Datenschutzbeauftragten / Vertreter in der EU

Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn …

die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder

die Kerntätigkeit des Verantwortlichen oder Auftragsverarbeiters in der umfangsreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 besteht.

Datenschutzbeauftragten / Vertreter in der EU

Der DSGVO unterliegende Organisationen haben einen Vertreter mit Sitz in der EU zu ernennen.

Wenn betroffenen Personen in der Union Waren od. Dienstleistungen angeboten werden.

Homepage / Datenschutzerklärung

Was Sie in Ihrer Datenschutzerklärung angeben müssen

1. Für welchen Zweck Sie die Daten verwenden. Webseitenanalyse, Newsletter,...
2. Kontaktdaten des Verantwortlichen oder Vertreters Name, E-Mail-Adresse, Telefon,...
3. Die Rechtsgrundlage Vertragserfüllung, Einwilligung, berechtigtes Interesse, ...
4. Ob Sie die Daten auch an Dritte übermitteln Cloud Speicher, Newsletter-Anbieter, Steuerberater, IT-Provider, ..

5. Ob Sie die Daten an Empfänger außerhalb der EU übermitteln und mit welchen Garantien, die Sicherheit der Daten gewährleistet wird Privacy Shield, Corporate Binding Rules,...

Zusammenfassung

- Informationspflicht / Dokumentationspflicht / Nachweispflicht

- Daten müssen angemessen geschützt werden

- Informieren und die Einwilligung der Person einholen, deren Daten verarbeitet werden

- "Privacy by design" und "Privacy by default" garantieren
- Einen Vertreter in der EU benennen
- Ein Verzeichnis der Verarbeitungstätigkeiten erstellen
- Verletzungen des Datenschutzes an die Aufsichtsbehörde melden
- Eine Datenschutz-Folgenabschätzung durchführen

Links

- **Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)**
  https://www.lda.bayern.de/de/index.html

- **Gesellschaft für Datenschutz und Datensicherheit**
  https://www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo

Fragen