PROBSTPARTNER

Neues Datenschutzrecht in der Schweiz und in der EU

Was man als Unternehmen wissen muss

Lunch and Law
Winterthur, 24. Januar 2018

Entwicklungen im Datenschutzrecht

- EU: Datenschutz-Grundverordnung («EU-DSGVO»)
- Schweiz: Revision Datenschutzgesetz («DSG»)

EU-DSGVO

- Inkrafttreten per 25. Mai 2016
- Umsetzungsfrist bis 25. Mai 2018

Zweck

Begriffe

Datenschutz
vs.
IT-Security

Personen-
bezogene Daten
vs.
Informationen
ohne
Personenbezug

Verarbeiten

Verantwortlicher

Auftragsverarbeiter

Personenbezogene Daten

1. „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

Verarbeitung

2. „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

Verantwortlicher/Auftragsverarbeiter

7. „Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

8. „Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

Räumlicher Anwendungsbereich

- Anwendbarkeit auch auf viele Schweizer Unternehmen, bspw.
  - Verarbeitung von personenbezogenen Daten erfolgt im Rahmen der Tätigkeit eines Verantwortlichen oder eines Auftragsbearbeiters in der EU, unabhängig davon, ob diese Verarbeitung in der EU stattfindet (Art. 3 Abs. 1 EU-DSGVO)
  - D.h. Verarbeitung veranlasst oder vorgenommen durch in der EU niedergelassenen Verantwortlichen oder Auftragsverarbeiter

Räumlicher Anwendungsbereich

- Anwendbarkeit auch auf viele Schweizer Unternehmen, bspw.
  - In CH wird Auffassung vertreten, DSGVO sei nicht auf schweizerische Unternehmen anwendbar, wenn und weil dieses als Auftragsverarbeiters eines Verantwortlichen mit Niederlassung in der EU tätig wird (oder umgekehrt) – ist aber letztlich nicht geklärt

Räumlicher Anwendungsbereich

- Betroffene Personen mit Aufenthalt in der EU, wenn Verarbeitung im Zusammenhang
  - Angebot von Waren und Dienstleistungen an betroffene Personen in der EU
    (bspw. Vertrieb von Waren über eine Webseite gezielt an natürliche Personen in der EU durch ein schweizerisches Unternehmen);

Räumlicher Anwendungsbereich

- Betroffene Personen mit Aufenthalt in der EU, wenn Verarbeitung im Zusammenhang
  - Beobachtung von Verhalten der betroffenen Personen, das in der EU erfolgt – hier wird argumentiert, dies sei nur anwendbar, wenn über Website oder App erfolge
    (bspw. Betrieb einer Webseite durch schweizerisches Unternehmen; betroffene Personen aus EU können sich registrieren und deren Verhalten wird personenbezogen aufgezeichnet und ausgewertet).

Sanktionen/Bussen

- In jedem «Einzelfall wirksam, verhältnismäßig und abschreckend»

- Je nach verletzter Bestimmung bis zu € 10 Mio. oder 2% des gesamten weltweiten Jahresumsatzes oder sogar € 20 Mio. oder 4% des gesamten weltweiten Jahresumsatzes (des Unternehmens)

Revision DSG

- Status: Entwurf liegt vor / parlamentarische Beratung als nächster Schritt

- Revisionsziele des Bundesrates:
  - Früheres Greifen des Datenschutzes;
  - Verstärkte Sensibilisierung der betroffenen Personen für die technologischen Risiken;
  - Erhöhung der Transparenz über Datenbearbeitungen;
  - **Anpassung an EU-Datenschutz-Grundverordnung & europ. Datenschutzkonvention**

Betroffenenrechte

- Rechte ausgebaut, u.a.:

Information (proaktiv)	Löschung	Einschränkung (EU)
Auskunft (auf Anfrage)	Widerspruch	Datenportabilität (EU)
Berichtigung		Sammelklage (EU)

- Betroffenenrechte = Pflichten der Unternehmen
- Voraussetzungen zur Pflichterfüllung schaffen

Massnahmen

Bearbeitungsverzeichnis erstellen
Prozesse aufsetzen für Auskunft / Löschung / Widerspruch etc.
Prozesse und Umsetzung dokumentieren
Schulung

Beispiel Auskunft

- Sie erhalten eine E-Mail von Absender kaj.seidl@gmx.com:

«Woher haben Sie meine Daten?!»

- Antwort geschuldet innert Monatsfrist
- Was tun?

1. Identifikation, Verifizierung des Anfragers
2. Erste Triage: Haben wir überhaupt Daten von dieser Person?
3. Zweite Triage: Schaffen wir die Auskunft innert Monatsfrist?
4. Intern: Alle vorhandenen Personendaten sammeln
5. Dritte Triage: Können wir die Auskunft allenfalls einschränken / verweigern?
6. Personendaten an Anfragenden schicken (wenn möglich elektronisch)

Schulung

Bearbeitungsverzeichnis

Prozesse

Bearbeitungsverzeichnis

Informationspflichten

- Diverse, detaillierte Informationspflichten, u.a. über:

Kontaktdaten	Auslandtransfer	Rechtsgrundlage (EU)
Zweck	Beschaffung von 3.	Dauer (EU)
Empfänger	Data Breach	Kontakt DS-Berater (EU)

- Heutige Information meist zu wenig detailliert

Massnahmen

Anpassung Datenschutzerklärungen
Anpassung Vertragstemplates (AGB, Arbeitsverträge)
Review Datenbeschaffungsprozesse (insb. Einkauf von Daten)
Prozess für Mitteilung einer Datenschutzverletzung (Data Breach)

Einwilligung

- Nicht jede Datenbearbeitung erfordert Einwilligung
- Eindeutig, freiwillig, informiert, jederzeit widerrufbar
- EU:
  - nicht möglich in AGB; nur noch Opt-In (keine prechecked Boxen)
- CH:
  - Teils möglich in AGB, teils nicht

Massnahmen

Review – Wo stütze ich mich auf Einwilligung?
Assessment – Nötig auch nach neuem Recht?
Anpassen der Einwilligungsprozesse (z. B. entfernen des «Häkchens»)
Prozess zur Umsetzung des Widerrufs

Auslagerung

- Auslagerung von Bearbeitung setzt Vertrag voraus
  - CH: ähnlich wie bisher nur Grundzüge vorgeschrieben
  - EU: detaillierte Vorschriften zu Mindestinhalt
    → EU Unternehmen werden dies als Auftraggeber einfordern!

Massnahmen

Review bestehender Auslagerungsverträge
(z.B. IT-Outsourcing, Cloud-Services, Callcenter, Werbeversand)
Anpassen der Verträge
Zusatzvereinbarungen

Weitere Neuerungen

- Datenschutzbeauftragter /-berater
- Data Breach Notification
- Datenschutzfolgenabschätzung
- Privacy by Design / Privacy by Default
- Ernennung eines Vertreters in der EU
- Datenportabilität («Data Portability»)
- AEE – Automatisierte Einzelentscheidung
- Codes of Conduct / Verhaltenskodizes

Das 2x3 der Datenschutz-Compliance

- 3 Grundsatzfragen
- 3 Umsetzungsschritte

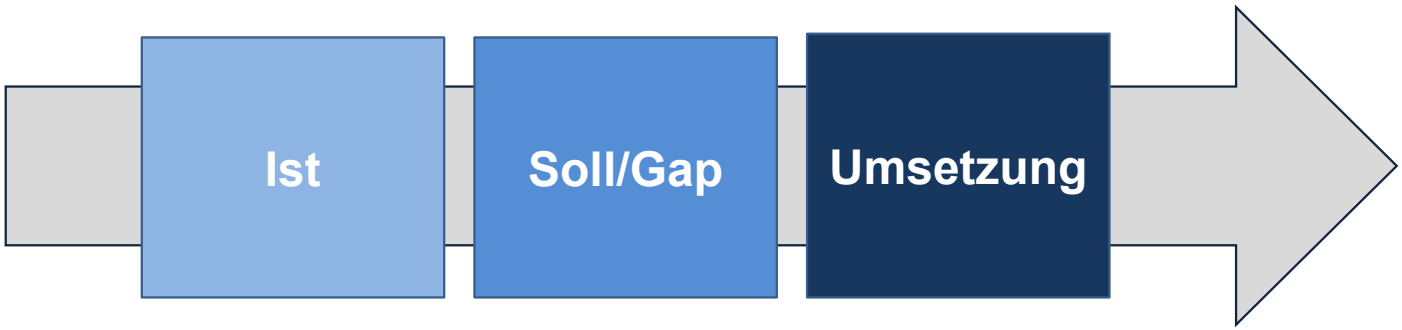
Grundsatzfragen

1. Ziele Datenschutz-Compliance:
   - als Marketinginstrument / Wettbewerbsvorteil?
   - zur Steuerung von Prozessen im Unternehmen?
   - nur minimal erforderliche Umsetzung?

2. Erwartungen

3. Schlüsselpersonen bestimmen und einbeziehen:
   - Verantwortlichkeiten identifizieren und bewusst machen
   - Wer übernimmt die Projektleitung?
   - externe Unterstützung?

3 Schritte zur Umsetzung



1. Aufnahme des Ist-Zustandes

- Ziel: Das Unternehmen hat einen Überblick über die bearbeiteten Personendaten und die damit verbundenen Risiken.

- Weg:
  - «Mapping»: Wer bearbeitet welche Personendaten zu welchen Zwecken auf welcher Grundlage und wie lange?
  - Welche Dokumentationen gibt es bereits?
  - Fragebogen, Feldarbeit

Proces B:		Check in
Process description:	Key process which includes general guest card management for the whole stay . Tre process contains not only check in of guest, filling of guest card and accommodation book but also any collecting of data in relation to beginning of guest´s stay as well as authorization of credit card.	
Personal data:	☒	Contact details I (name, surname, address)
	☒	Contact details II (e-mail, phone number, IP)
	☒	Age
	☒	Birth number/Birth date
	☒	Sex
	☒	Nationality
	☒	Credit card data
	☒	Identification document
	☒	Number plate
	☒	Third parties data (accompanying persons)
	☒	Social anamnesis (senior, employee)
	☒	Other: purpose of stay
Storage:		Email server
	☒	IS Accommodation
	☒	Central archive
		IS Oracle
	☒	Card file reception
	☒	Local archive
		Other: .....
Access rights:	☒	Reception
	☒	Head of reception
	☒	Accommodation office
	☒	Marketing/sales
	☒	Accounting department
	☒	IT department
	☒	Other: general management
Processor:	No	

2. Soll/Gap Compliance Analyse

- Ziel: Anpassungsbedarf evaluieren, Festlegung der Massnahmen und Umsetzungsplanung.

- Weg:
  - Prüfung der Datenbearbeitungen auf Datenschutzkonformität und Schwachstellen
  - Evaluation Anpassungsbedarf
  - Identifikation der Umsetzungsmassnahmen
  - Priorisierung und Planung

Können Sie Bewerberdaten im Falle eines Löschungsbegehrens von Ihren Systemen löschen und alle gedruckten Dossiers vernichten?

Können Sie einem Mitarbeiter oder Kunden Auskunft über die über ihn bearbeiteten Personendaten erteilen?

3. Umsetzung

- Ziel: Identifizierte Massnahmen sind umgesetzt, Einhaltung des Datenschutzes ist dokumentiert.

- Weg:
  - Datenschutzstelle intern und/oder extern
  - Reglemente und Prozesse zum Datenschutz
  - Datenbearbeitungsverzeichnis
  - Abschluss / Anpassung von Verträgen
  - Informationspflichten / Datenschutzerklärungen
  - Datenschutz-Folgenabschätzung
  - Kommunikation und Schulung Mitarbeiter

Process Abbreviation	*C17*	Joint Controllers		Storage Duration	*forever*
Process Name	*Marketing: Newsletter*	Child´s Data		Nature of Processing	*automatic*
Previous Process	*B6; C3*	Special Categories of Data		Process Owner	*Mrs. Suchá*
Following Process	*none*	New Purpose	x	Legal Title	*legitimate interest*
Data Processed	*email address; name; sex*	Profiling	x	Legal Obligation	*none*
Purpose	*marketing - offer of services*	Specific Processing Situation		Legitimate Interest	*direct marketing*
Origin/Source	*data subject; bookings; travel agencies*	Right to Data Portability		Soft Regulation	*none*
Processor	*marketing agency (contract)*	Cross-Border Processing	x	Country	*EU*
Recipients	*holding*	Transfer to 3. Countries		Country	
Virtual Storage	*email server, CRM*	Adequacy Decision		Other Transfer Title	
Physical Storage	*none*				
Risk Assessment	*43*				

zu guter Letzt

- Herausforderungen:
  - Zusammentragen der erforderlichen Informationen
  - fehlende personelle Ressourcen
  - Anpassung von IT-Systemen und Geschäftsprozessen

- risikobasierter Ansatz

- Projekt muss von Unternehmensleitung getragen werden (sie tragen auch die Verantwortung und Folgen)


Vielleicht wenn ich mich hier hinsetze und auf die Sumpfhühner starre, die im Sumpf rumsumpfen, vermeide ich allen Ärger.

bei weiteren Fragen

www.swissdataprotectionlaw.ch