

Neues Datenschutzrecht ab 01.09.2023

Fachreferat

Dr. Hans R. Schibli, Rechtskonsulent / Vizepräsident



Aargauischer Gewerbeverband

Inhalt

1. Anwendungsbereich
2. Grundsätze
3. Strafandrohungen
4. Grundregeln für Geschäfte
5. Grundregeln für Mitarbeitende
6. Fragerunde

Anwendungsbereich

- Bearbeitung von Personendaten von natürlichen Personen
 - Daten von AG, GmbH, Vereinen und Stiftungen sind aus DSGVO-Sicht nicht problematisch.
- Bearbeitung durch uns alle (ausser als Private)
 - Einzelfirmen
 - AG, GmbH, Genossenschaften, Kollektiv- und Kommanditgesellschaften
 - Vereine, Verbände, Stiftungen
- Relevante Artikel im DSGVO und DSV
 - Art. 5 – 13 (Art. 14 – 18 nur bei Auslandsbezug) DSGVO
 - Art. 19 – 32 sowie Art. 60 – 66 DSGVO
 - Art. 1 – 24 DSV

Grundsätze (Art. 6)

- Rechtmässige Bearbeitung erlaubt (Vertrag, Gesetz, Einwilligung)
- Zweckorientierung
- Verhältnismässigkeitsprinzip
- Vernichtung/Anonymisierung wenn Zweck erreicht

Strafandrohungen

- Busse bis CHF 250'000
- vorsätzlich
- auf Antrag (3 Monate ab Kenntnis vom „Täter“).
- Bis zu CHF 50'000 kann der Geschäftsbetrieb anstelle der Chefs/Verantwortlichen verurteilt werden.
- Strafverfolgung: 5 Jahre

Lösung: Datenschutz ernst nehmen, nicht
 hyperventilieren
 Fahrlässiges Handeln ist nicht strafbar

Grundregeln für Geschäfte

Pflichten für KMU (1)

- Verwendung Daten nur für den Zweck und solange Zweck besteht (rechtmässige Verwendung)

Lösung: Datenschutzweisung (Muster-Beilage)

Pflichten für KMU (2)

- Korrektheit, Vollständigkeit und Aktualität der Daten
→ Kundendaten (im eigenen Interesse des KMU)

Lösung: Datenschutzerklärung (Muster-Beilage)
ev. Ernennung Datenschutzbeauftragter

→ Mitarbeitendendaten

Lösung: In Arbeitsvertrag Klausel aufnehmen (Beilage)

Pflichten für KMU (3)

- Organisation der Datenbearbeitung, nach Stand der Technik und verhältnismässig (Art. 7 DSGVO; Art. 3 DSV)
 - Vertraulichkeit (Zugriffskontrolle Zugangskontrolle, Benutzerkontrolle)
 - Verfügbarkeit (Datenträger, Speicher, Wiederherstellung, etc.)
 - Nachvollziehbarkeit

Lösung: wird automatisch gemacht. Zudem

- Verschwiegenheitspflicht in Arbeitsvertrag (Beilage)
- Datenschutzweisung (Muster-Beilage)
- Schulung Mitarbeitende (regelmässig)
- Delegation an Schlüsselerantwortlicher
- Delegation an IT-Unternehmen / Software, wenn Probleme → Meldung an EDÖB

Pflichten für KMU (3a)

Privacy by Design (Art. 7 Abs. 1)

- Datenschutz ist in der frühestmöglichen Phase der Planung zu berücksichtigen (durch Ergreifen von TOM's – techn./org.Massnahmen)
 - Beispiel neues CNC-Gerät: Datenmigration/-sammlung
 - Beispiel Lieferwagenkauf: Thema Mitarbeiterüberwachung
 - Beispiel: Rabattkarten(-systeme): Kundendaten
 - Beispiel: Einstellungsprozess

Lösung: Ernennung Datenschutzbeauftragter
Datenschutzweisung

Pflichten für KMU (3b)

Privacy by Default (Art. 7 Abs. 3)

- Werkeinstellungen datenschutzfreundlich
 - Beispiel Homepage: Newsletter-Button
 - Beispiel Auftrag: zu breite Definition des Zwecks
 - Beispiel neues Fahrzeug: zentrale Überwachung

Pflichten für KMU (4)

- Verzeichnis der Bearbeitungstätigkeiten
 - Wenn mehr als 250 Mitarbeitende, oder
 - Wenn besonders schützenswerte Personendaten in grossem Umfang bearbeitet werden (Apotheke, Arzt, Strafverteidiger)

Lösung: Verzeichnis gemäss Anhang zur Datenschutzweisung ausfüllen.

Pflichten für KMU (5)

- Pflicht, die betroffene Person über die Datenbearbeitung zu informieren (Art. 19).

Lösung: Datenschutzerklärung auf Website
AGB, Auftragsbestätigung
Anhang zum Arbeitsvertrag

- Datenschutz-Folgenabschätzung zu erstellen
 - Wenn besonders schützenswerte Personendaten in grossem Umfang bearbeitet werden (Apotheke, Arzt, Strafverteidiger)

Lösung: Weisung (Beilage) in Kraft setzen
Bei Bedarf Folgen-Abschätzung erstellen.

Möglichkeiten

- Bearbeitung der Daten durch Auftragsbearbeiter (externe Firma)
- Datenschutzberater: Anlaufstelle für betroffene Personen und die Behörden.

Lösung: Auftragsbearbeitungsvertrag erstellen (Muster anbei).

Auskunftsrecht (Art. 25 DSGVO)

- Über alle Daten
- Innerhalb 30 Tagen seit Anfrage
- Man kann nicht auf dieses Recht im Voraus (AGB) verzichten
- Unentgeltlichkeit

Lösung: ev. Person bezeichnen in der Firma
Mitarbeitende → Personalabteilung;
Kunden → Kundenservice / Verkauf

Herausgaberecht

(Art. 28 DSGVO, Art. 16 ff. DSV)

- Grundsätzlich immer (Art. 16 ff. DSV)
- Zudem Anspruch auf die Herausgabe in einem gängigen elektronischen Format, wenn
 - Verantwortlicher bearbeitet die Daten automatisiert (→ ESR Zahlungen)
 - Einwilligung zur Bearbeitung oder vorbestehende Vertragsbeziehung

Grundregeln für Mitarbeitende

Grundregeln für Mitarbeitende

- Datenschutz ist Persönlichkeitsschutz
 - Schutz der Privatsphäre von Menschen
 - Schutz vor Persönlichkeitsverletzungen durch missbräuchliche Datenbearbeitung oder Falschinformationen

- Personenbezogene Daten (= Personendaten) sind alle Informationen, die sich auf einen bestimmten Menschen beziehen

1. Schweigen ist Gold

- Was ich über Kunden, Angestellte und Chefs erfahre → bleibt bei mir
- Ich rede mit niemandem über Kunden und Mitarbeitende meines Arbeitgebers
 - Beispiel: Chef hat Burnout
 - Beispiel: Kunde geht in Konkurs
 - Beispiel: Angestellter wird während Arbeitszeit am Kiffen gesehen

Lösung: Einwilligung des Dateninhabers
Informationen sind öffentlich
vorbestehende Verträge

2. Besprechungen sind vertraulich

- Gespräche mit Arbeitskollegen / geschäftliche Besprechungen: Feind hört mit!
 - SBB 1. Klasse Bern-Zürich
 - Auto-Freisprechanlage
 - Migros, Coop, Golfplatz, Restaurant
 - Face-Book

Lösung: Anonymisieren

3. Arbeitsplatz ist sauber

- Offen herumliegende Informationen sind wie ein unsauberer Arbeitsplatz → Sicherheitsrisiko
 - Gilt für den physischen Arbeitsplatz (offene Kundenbestellungen, korrekte Entsorgung)
 - Gilt für den digitalen Arbeitsplatz (nicht gesperrter Bildschirm; ungeschützte USB-Sticks)
 - Gilt bei jedem Verlassen des Arbeitsplatzes (WC, Pause, etc), gilt auch zuhause / unterwegs

Lösung: Schulungen / Sensibilisierung gegenseitig!

Diskussion & Fragen

Dr. Hans R. Schibli

h.schibli@agv.ch

hans.r.schibli@schibli-partner.ch