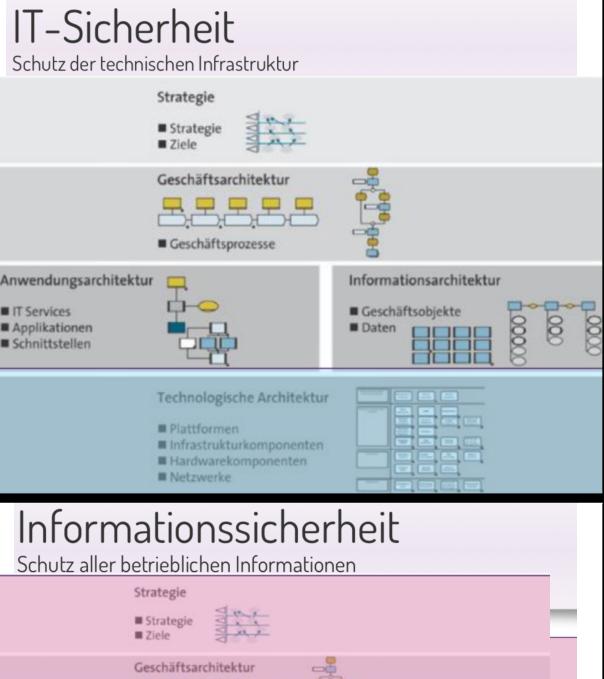
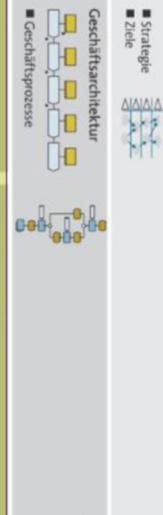


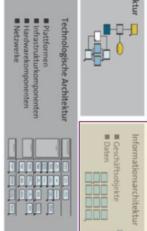
Datensicherheit

Schutz der Geschäftsdaten (inkl. der Systeme zu deren Bearbeitung)



Datenschutz

Schutz von Personendaten (im Sinne von Persönlichkeitssprofilen)



Thema	Neues DSG	DSGVO
Benennen eines Datenschutzauftragten	Keine Pflicht, aber empfohlen.	Pflicht gemäß Art. 37 DSGVO.
Melden von Datenschutzverletzungen	Pflicht, möglichst rasch zu melden.	Pflicht, innerhalb 72 Stunden zu melden.
Sanktionen	Bussen bis zu EUR 20 Mio. oder 4% des weltweiten Gesamtjahresatzes des Unternehmens.	Bussen bis zu CHF 250'000 für verantwortliche private Personen.
Informationspflicht	Geringe inhaltliche Vorgaben für Datenschutzrichtlinien. Es sind aber alle Länder aufzuführen, in die Personendaten übermittelt werden.	Minimale Inhaltsvorgaben für Datenschutzrichtlinien gemäß Art. 13 DSGVO.
Datenexporte	Über die Zulässigkeit entscheidet der Bundesrat. Es sind dieselben Standardvertragsklauseln und verbindlichen unternehmensinternen Vorschriften wie in der EU anwendbar.	Über die Zulässigkeit entscheidet die Europäische Kommission. Standardvertragsklauseln, verbindliche unternehmensinterne Vorschriften.
Verzeichnis der Verarbeitungstätigkeiten	Neu mit Angabe des Ziellands bei Datenexport.	Gemäß Art. 30 DSGVO.
Datenschutz-Folgenabschätzung	Rücksprache mit einem Datenschutzauftragten oder dem EDÖB ist möglich, wenn trotz Massnahmen ein hohes Risiko besteht.	Rücksprache mit Aufsichtsbehörden ist obligatorisch, wenn trotz Massnahmen ein hohes Risiko besteht.

Confidentiality (Vertraulichkeit)

Leitfrage:

Wer darf auf welche Daten in welchem Umfang und unter welchen Voraussetzungen zugreifen?

Vertraulichkeit ist gegeben, wenn nur Berechtigte bestimmte Daten sehen und nutzen können.

Beispiele für Massnahmen:

- Ständige Kontrolle, ob nur Befugte bestimmte Daten verarbeiten können (Zugriffsmangement).
- Verschlüsselte Datenübertragung.
- Sicheres Löschen der Daten und ein Entsorgungskonzept für Datenträger.

Integrity (Integrität)

Leitfrage:

Wie kann die Verlässlichkeit der Daten oder Informationen dauernd Gewährleistet werden?

- Ein System ist dann integer, wenn Daten während der Datenverarbeitung unversehrt, vollständig und aktuell bleiben.

Beispiele für Massnahmen:

- Ständige Kontrolle, durch Protokollierung.
- Digitale Signatur.
- Hashes als «Fingerabdruck» von Dateien.

Availability (Verfügbarkeit)

Leitfrage:

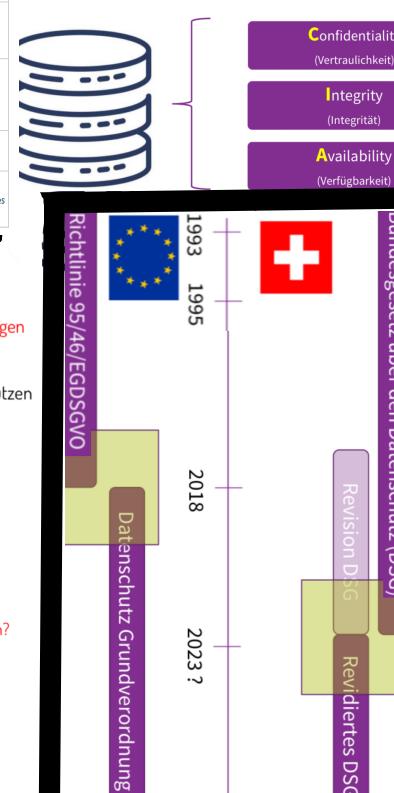
Sind die Informationen zugänglich, wann und wo sie von den Berechtigten gebraucht werden?

Verfügbarkeit ist gegeben, wenn die Daten/Informationen zur rechten Zeit am rechten Ort genutzt werden können.

Beispiele für Massnahmen:

- Zentrale Speicherung der Daten.
- Redundanz schaffen.
- Backup.

Die Schutzziele bezogen aus Sicht Datensicherheit



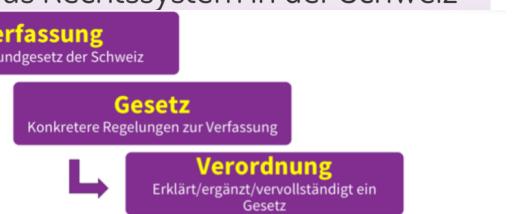
Zusammenfassung

	Datensicherheit	Datenschutz
Ziel	Schutz aller betriebsrelevanten Daten	Schutz der Persönlichkeit von Menschen
Motivation	Fortbestand des Unternehmens	Per Gesetz verordnet
Primär verfolgte Schutzziele	C, I, A	C, I
Betroffene	Jedes Unternehmen (und natürlich auch Privatpersonen)	Unternehmen und Private, welche personenbezogene Daten sammeln und/oder bearbeiten

Beispiel: Schutzbedarfsanalyse für die HR-Applikation eines Betriebs

Anwendungen		Schutzbedarfsfeststellung		
Nr.	Beschreibung	Grundwert	Schutzbedarf	Begründung
A1	Personalverwaltung	Vertraulichkeit	Hoch	DSG
		Integrität	Normal	Fehler können rasch erkannt werden
		Verfügbarkeit	Normal	Ausfall bis zu mehreren Tagen möglich

Das Rechtssystem in der Schweiz



Relevantes Recht für die IT-Branche

Privatrecht

- OR (Obligationenrecht)
- DSG (Datenschutzgesetz) und VDSG (Verordnung zum DSG)
- URG (Urheberrechtsgesetz)

Öffentliches Recht

- StGB (Strafgesetzbuch)
- FMG (Fermladegesetz)
- ZertES (Bundesgesetz über elektronische Zertifizierungsdienste)
- BUPF (Bundesgesetz zur Überwachung des Post- und Fernmeldeverkehrs)

Modelle:

- Copyright
- Public Domain
- Fair Use
- Creative Commons

Zweck und Geltungsbereich

Art. 1 Zweck

Dieses Gesetz bezieht den **Schutz der Persönlichkeit** und der Grundrechte von Personen, über die Daten bearbeitet werden.

Art. 2 Geltungsbereich

1 Dieses Gesetz gilt für das Bearbeiten von Daten **natürlicher und juristischer** Personen durch:

- a. private Personen;
- b. Bundesorgane.

Datenbeschaffung und -bearbeitung

3 Personendaten dürfen **nur zu dem Zweck** bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.

4 Die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung müssen **für die betroffene Person erkennbar** sein.⁸

5 Ist für die Bearbeitung von Personendaten die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung erst gültig, wenn sie nach angemessener Information freiwillig erfolgt. Bei der Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen **muss die Einwilligung zudem ausdrücklich erfolgen**.⁹

Auskunftsrecht und Datensicherheit

Art. 8 Auskunftsrecht

1 **Tede Person** kann vom Inhaber einer Datensammlung Auskunft darüber verlangen, ob Daten über sie bearbeitet werden.

Art. 7 Datensicherheit

1 Personendaten müssen durch **angemessene technische und organisatorische** Massnahmen gegen unbefugtes Bearbeiten geschützt werden.

2 Der Bundesrat erlässt nähere Bestimmungen über die Mindestanforderungen an die Datensicherheit.

Anmeldung und Meldepflicht von Datensammlungen

2 **Bundesorgane müssen sämtliche Datensammlungen** beim Beauftragten zur Registrierung anmelden.

3 **Private Personen** müssen Datensammlungen anmelden, wenn:

- a. **regelmäßig besonders schützenswerte Personendaten** oder Persönlichkeitsprofile bearbeitet werden; oder
- b. regelmäßige Personendaten an Dritte bekannt gegeben werden.

4 Die Datensammlungen müssen angemeldet werden, bevor sie eröffnet werden.

Besonders schützenswerte Personendaten und Persönlichkeitsprofil

besonders schützenswerte Personendaten: Daten über:

1. die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten,
2. die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit,
3. Massnahmen der sozialen Hilfe,
4. administrative oder strafrechtliche Verfolgungen und Sanktionen;

Persönlichkeitsprofil: eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt;

VDSG: Reglement und Protokollierung

Für besonders schützenswerte Personendaten oder für Persönlichkeitsprofile gilt gemäß VDSG zusätzlich:

Art. 10 - Protokollierung:

- Der Inhaber der Datensammlung protokolliert die automatisierte Bearbeitung.
- Die Protokolle sind während eines Jahres revisionsgerecht festzuhalten.

Art. 11 - Bearbeitungsreglement:

- Das Bearbeitungsreglement enthält insbesondere die interne Organisation, sowie das Datenbearbeitungs- und Kontrollverfahren.
- Es umschreibt die Unterlagen über die Planung, die Realisierung und den Betrieb der Datensammlung und der eingesetzten Informatikmittel.

Änderungen mit dem revidierten DSG (1)

Geltungsbereich:

- Gilt nur noch für natürliche Personen (juristische Personen fallen weg)

Informations- und Transparenzpflichten:

- Generelle Datenschutzerklärung (Informationspflicht)
- Keine generelle Einwilligung beim Profiling, jedoch eine Einwilligung bei hohen Risiken, wie momentan bei Persönlichkeitsprofilen

Höhere Sorgfaltspflichten:

- Pflicht zur Dokumentation der Datenbearbeitung.
- Bearbeitungsgrundsätze «**Privacy by Design**» und «**Privacy by Default**».

Änderungen mit dem revidierten DSG (2)

Weitere Änderungen:

- Ausgebautes Auskunftsrecht.
- Datenfolgeabschätzungen (Bei heiklen Personendaten)
- Meldepflicht bei Datenschutzverletzungen

Stärkere und bessere Aufsicht:

- Der «**Edigenössische Datenschutzbeauftragte EDÖB** kann Verfügungen aussprechen (jedoch keine Bussen verhängen).
- Der Bundesrat legt Länder mit «**angemessenem Datenschutz** fest.
- Pro Vorfall können Strafen bis Fr. 250'000.- ausgesprochen werden (im Vergleich: EU-DSGVO sogar bis EUR 20'000'000.- oder 4% des Jahresumsatzes)

VÜPF: Verordnung über die Überwachung des Post- und Fernmeldeverkehrs

BÜPF: Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs

Surfen im Internet nach dem Inkrafttreten der DSGVO

Wie möchten Sie FAZ.NET nutzen?

Wie gewohnt mit Werbung lesen

Nutzen Sie FAZ.NET mit personalisierter Werbung, Werbetracking, Nutzungsanalyse und externen Multimedia-Inhalten. Details zu Cookies und Verarbeitungszwecken sowie zu Ihren jederzeitigen Widerentspruchsmöglichkeiten finden Sie unten, im [Cookie-Manager](#) sowie in unserer [Datenschutzerklärung](#).

EINVERSTÄNDEN

Erfahren Sie mehr in den [FAQs](#).

Werbefrei mit FAZ.Z. Pur lesen

Lesen Sie FAZ.NET fokussiert ohne Werbung und ohne Werbetracking für 4,99 € pro Monat. Schließen Sie jetzt das FAZ.Z. Pur Abo ab.

WERBEFREI LESEN

Sie beziehen bereits ein FAZ.Z. Pur Abo? Hier anmelden.

*Für die Nutzung mit Werbung und Cookies: Wir, die Frankfurter Allgemeine Zeitung GmbH und unsere Partner, verarbeiten Daten (Informationen wie Cookies, Gerät-Kennungen, IP-Adresse) für unten näher beschriebene Zwecke. Es werden Informationen auf Ihrem Gerät gespeichert und abgerufen. Durch das Klicken des „Einverständnis“-Buttons stimmen Sie dieser Verarbeitung zu. Darüber hinaus willigen Sie gemäß Art. 49 Abs. 1 DSGVO ein, dass die Partner die Daten gegebenenfalls auch in Drittlanden verarbeiten, in denen kein vergleichbares Datenschutzniveau vorherrscht (z.B. in den USA). In solchen Fällen ist es etwa möglich, dass Behörden dieser Drittländer auf den Daten Zugriff nehmen.

Verarbeitungszwecke

- > Informationen auf einem Gerät speichern und/oder abrufen
- > Personalisierte Anzeigen und Inhalte, Anzeigen- und Inhaltsmessungen, Erkenntnisse über Zielgruppen und Produktentwicklungen
- > Einbindung von externen Multimedia-Inhalten

Einverständniserklärung

*Für die Nutzung mit Werbung und Cookies: Wir, die Frankfurter Allgemeine Zeitung GmbH und unsere Partner, verarbeiten Daten (Informationen wie Cookies, Gerät-Kennungen, IP-Adresse) für unten näher beschriebene Zwecke. Es werden Informationen auf Ihrem Gerät gespeichert und abgerufen. Durch das Klicken des „Einverständnis“-Buttons stimmen Sie dieser Verarbeitung zu. Darüber hinaus willigen Sie gemäß Art. 49 Abs. 1 DSGVO ein, dass die Partner die Daten gegebenenfalls auch in Drittlanden verarbeiten, in denen kein vergleichbares Datenschutzniveau vorherrscht (z.B. in den USA). In solchen Fällen ist es etwa möglich, dass Behörden dieser Drittländer auf den Daten Zugriff nehmen.

Informationspflicht nach DSGVO

Wer «steckt» hinter der Webseite
(Anbieterkennung)

Impressum

Was wird mit den Daten gemacht?
(Datenschutzerklärung)

Datenschutz-Erklärung

Welche Rechte hat der Verbraucher?
(Cookie-Einstellungen, etc.)

Nur technisch notwendige

Anpassen

Alle akzeptieren

Externe Links

Probleme:

- Urheberrecht...
- Unlauterer Wettbewerb...
- Links auf rechtswidrige oder strafbare Inhalte...

Lösungsansätze:

- Klare Markierung von externen Links...
- Disclaimer (Wirkung juristisch umstritten)

Allgemeine Geschäftsbedingungen

(Schweizerisches Recht)

Allgemeine Geschäftsbedingungen (AGB) sind vorformulierte Vertragsklauseln. Man spricht auch von «kleingedruckten». Die (wirtschaftlich stärkeren) Anbieter wollen damit die Verträge mit ihren (privaten) Kunden vereinfachen und rationell gestalten.

Damit AGB Bestandteil eines Vertrags werden, muss der Kunde sie bei Vertragsabschluss zur Kenntnis nehmen. Der Anbieter muss sie also übergeben oder in geeigneter Form auf sie hinweisen, indem er sie zum Beispiel in seinen Geschäftsräumen unüberhörbar aufhängt oder auflegt. Beim Online-Shopping sind die Kunden in der Regel aufgefordert, ein Häkchen zu setzen und so zu bestätigen, dass sie die AGB gelesen haben und akzeptieren.

In den AGB sind die gegenseitigen Rechte und Pflichten der Vertragsparteien festgehalten. Da in der Schweiz Vertragsfreiheit besteht, haben AGB sehr oft Vorrang vor gesetzlichen Bestimmungen. Das kann dazu führen, dass Kunden und Kunden beim Akzeptieren von AGB auf Rechte, die ihnen das Gesetz zugestellt würde, verzichten.

Wofür werden Cookies eingesetzt?

- Identifizierung des Surfers ([Session ID](#))
- Abspeichern eines [Logins](#) bei einer [Webanwendung](#)
- Abspeichern eines [Warenkorbs](#) bei einem [Online-Händler](#)
- [Webtracking](#) von Nutzern

Der Begriff **Cookie** wird im Datenschutz auch als Synonym für Datenentnahme, Datenspeicherung, Datennutzung, Datenverwertung, Datenweitergabe wie auch Datenmissbrauch verwendet, unabhängig davon, ob dazu tatsächlich ein physisches Cookie verwendet wird oder andere Techniken eingesetzt werden.

Zusätzliche Angaben auf Webseiten

Welche Regeln gelten beim Geschäft (z.B. im WebShop)?
(Zahlungsfristen, Lieferung, Gerichtsstand, etc.)

Allgemeine Geschäftsbedingungen (AGB)

Externe Links
(Urheberrecht, Distanzierung von fremden Inhalten)

Disclaimer

Was sind Cookies?

Zusammenfassung aus Wikipedia (gekürzt):

Ein **Cookie** ist eine [Textinformation](#), die im [Browser](#) auf dem Endgerät des Betrachters zu einer besuchten [Website](#) gespeichert werden kann.

Das Cookie wird entweder vom Webserver an den Browser gesendet oder im Browser von einem Skript erzeugt.

Der Webserver kann bei späteren, erneuten Besuchen dieser Seite diese Cookie-Information auslesen oder über ein Skript der Website die Cookie-Information an den Server übertragen.

Warum sind Cookies heikel?

Die Rechtslage bei der Nutzung von Analytic-Tools ist gegenwärtig umstritten.

Rechtlicher Anstoß für die Kritik ist das [Speichern der IP-Adresse](#) beim Verwenden von Cookies.

Das Datenschutzgesetz lässt die Erhebung und die Speicherung von [persönbezogenen Daten](#) nur dann zu, wenn dies von einer gesetzlichen Vorschrift explizit erlaubt wird oder eine eindeutige und vorherige Einwilligung des Nutzers vorliegt.

Das [Speichern von IP-Adressen bedarf einer Rechtsgrundlage nach DSGVO](#)

Eine Speicherung oder Verarbeitung der IP-Adresse [über den Nutzungsvertrag hinaus](#) benötigt immer eine rechtliche Grundlage des Art. 6 DSGVO.

Das DSG regelt den Datenschutz sowohl für staatliche wie private Datenverantwortliche. Obwohl es von der DSGVO inspiriert wurde und wesentliche Bestimmungen repliziert, ist das DSG gegenüber der DSGVO deutlich weniger detailliert.

Datenschutzerklärung (Ausschnitt)

Frankfurter Allgemeine Zeitung GmbH

Hellerhofstraße 2-4

60327 Frankfurt am Main

Tel.: 0049 (0)69 7591-0

E-Mail: Info@faz.net

Handelsregister: HRB 7344

Amtsgericht Frankfurt am Main Ust.-IDNr.: DE 114 232 723

Steuer-Nr.: 045 227 77055

Geschäftsführer:

Thomas Lindner (Vorsitzender), Dr. Volker Breid

Herausgegeben von:

Gerald Braunberger, Jürgen Kaube, Carsten Knop, Berthold Kohler

Fair Use

Was ist Public Domain? Werden man im Internet auf den Ausdruck «Fair Use»

Werk denkt, dass damit gekennzeichnete Ressourcen für nicht kommerzielle Projekte verwendet werden können, der irrt sich.

Der Begriff Public Domain kommt aus Zentral- und Nordamerika, insbesondere für bildende und künstlerische Zwecke eingesetzt werden.

Was ist Public Domain? Als Public Domain wird die urheberfreie Gemeinfreiheit von Dateien wie Musikstücken, Bildern oder aber ganze Software bezeichnet.

Alles, was zur Public Domain gehört, darf von jeder Person ohne irgendwelche Restriktionen genutzt werden.

Der Begriff Public Domain kommt aus Zentral- und Nordamerika, insbesondere in den USA.

In Deutschland und den meisten anderen Staaten kann ein Urheber nicht komplett auf das Urheberrecht verzichten.

Copyright Die Entscheidung, ob und wofür andere ein bestimmtes Werk verwenden dürfen, liegt beim Ersteller bzw. beim Autor. Ganzässiglich können Werke kostenlos oder kostenpflichtig zur Verfügung stehen.

lediglich gilt: Auch wenn man Geld für eine Ressource bezahlt, heißt das nicht automatisch, dass man diese uneingeschränkt eingesetzen darf. Der Schöpfer einer Ressource kann entscheiden, ob und wofür sein Eigentum verwendet