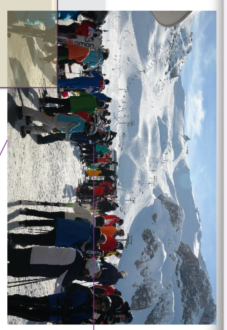
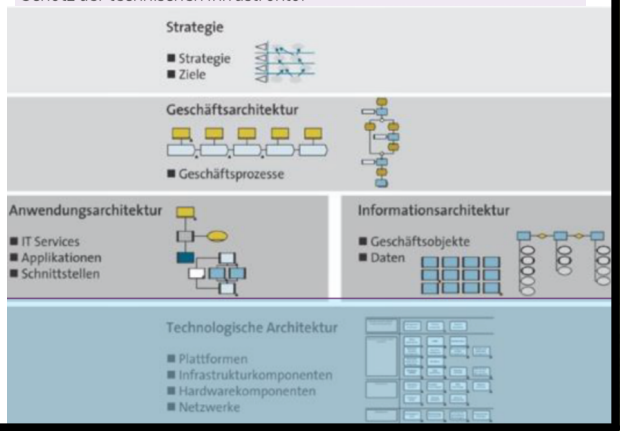
Datenschutz

Schutz von Personendaten (im Sinne von Persönlichkeitsprofilen)



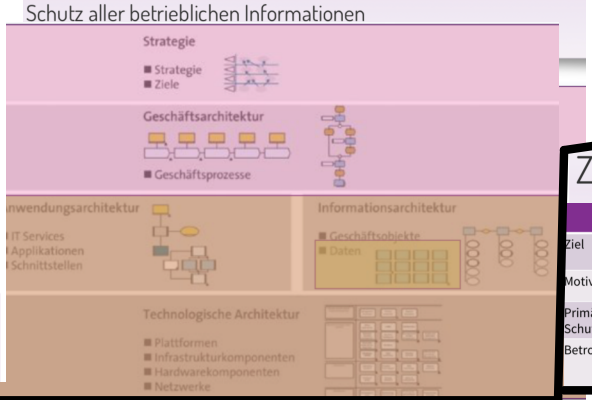
IT-Sicherheit

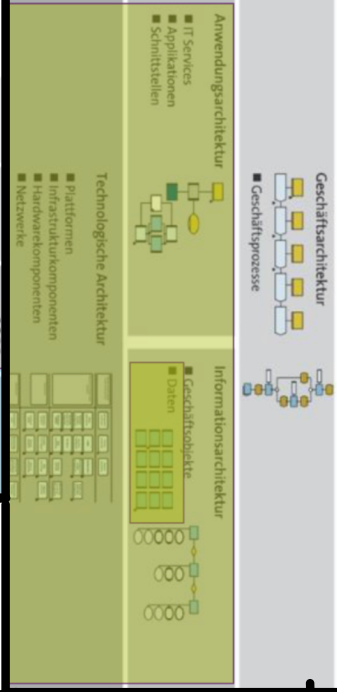
Schutz der technischen Infrastruktur



Informationssicherheit

Schutz aller betrieblichen Informationen





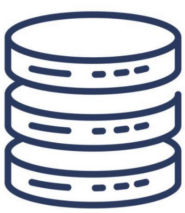
Datensicherheit

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

Zusammenfassung

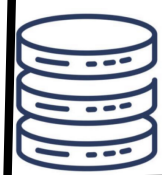
	Datensicherheit	Datenschutz
Ziel	Schutz aller betriebsrelevanten Daten	Schutz der Persönlichkeit von Menschen
Motivation	Fortbestand des Unternehmens	Per Gesetz verordnet
Primär verfolgte Schutzziele	C, I, A	C, I
Betroffene	Jedes Unternehmen (und natürlich auch Privatpersonen)	Unternehmen und Private,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

Die Schutzziele CIA



- **C**onfidentiality (Vertraulichkeit)
- **I**ntegrity (Integrität)
- **A**vailability (Verfügbarkeit)

Die Schutzziele bezogen aus Sicht Datensicherheit



- **C**onfidentiality (Vertraulichkeit)
- **I**ntegrity (Integrität)
- **A**vailability (Verfügbarkeit)

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

Legende		
Normal (Schaden begrenzt)	**Hoch** (Schaden beträchtlich)	**Sehr hoch** (Schaden existenziell)
Von BSI IT-Grundschutz abgedeckt	BSI IT-Grundschutz bildet Basisschutz, reicht evtl. nicht aus (Risikoanalyse)	BSI IT-Grundschutz bildet Basisschutz, reicht in der Regel nicht aus (Risikoanalyse)

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 (Zugriffsmanagement).
- 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.

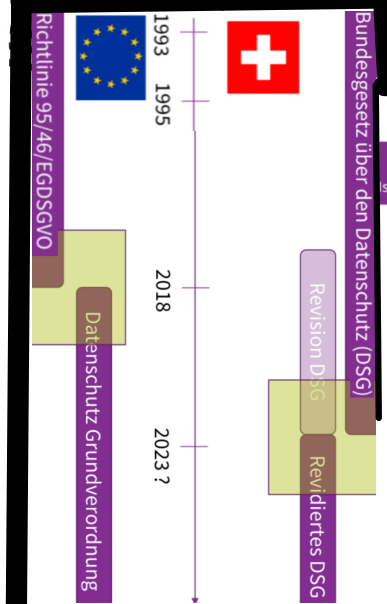
Beispiele für Massnahmen:
- Ständige Kontrolle, durch Protokollierung.
- Digitale Signatur.
- Hashes als «Fingerabdruck» von Dateien.

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.



Lizenzierungsmodelle für Webseiteninhalte

Modelle:
- Copyright
- Public Domain
- Fair Use
- Creative Commons

Das Rechtssystem in der Schweiz

Verfassung
ist das Grundgesetz der Schweiz

↳ **Gesetz**
Konkretere Regelungen zur Verfassung

↳ **Verordnung**
Erklärt/ergänzt/vervollständigt ein Gesetz

↳ **Reglement**
Präzise Einzelbestimmungen zur Verordnung

Relevantes Recht für die IT-Branche

Privatrecht (Verhältnis zwischen natürlichen und juristischen Personen)
- OR (Obligationenrecht)
- DSG (Datenschutzgesetz) und VDSG (Verordnung zum DSG)
- URG (Urheberrechtsgesetz)

Öffentliches Recht (Verhältnis zwischen Staat und natürlichen oder juristischen Personen)
- StGB (Strafgesetzbuch)
- FMG (Fernmeldegesetz)
- ZertES (Bundesgesetz über elektronische Zertifizierungsdienste)
- BÜPF (Bundesgesetz zur Überwachung des Post- und Fernmeldeverkehrs

Zweck und Geltungsbereich

Art. 1 Zweck

Dieses Gesetz bezweckt 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] Jede 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. regelmässig 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

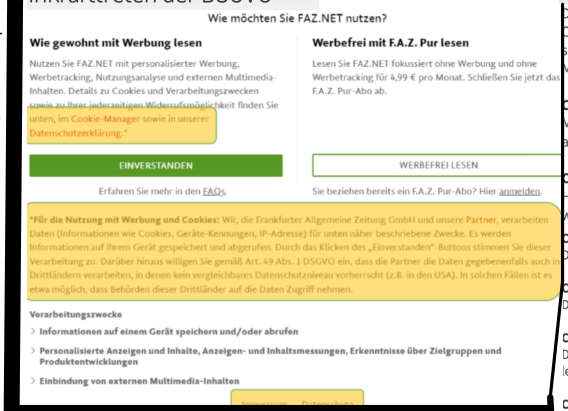
Höhere Sorgfaltspflichten:
- Pflicht zur Dokumentation der Datenbearbeitung.
- Bearbeitungsgrundsätze **«Privacy by Design»** und **«Privacy by Default»**.

Änderungen mit dem revidierten DSG (2)

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

Stärkere und bessere Aufsicht:
- Der «Eidgenössische Datenschutzbeauftragte EDÖB kann Verfügungen aussprechen (jedoch keine Bussen verteilen).
- 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)

Surfen im Internet nach dem Inkrafttreten der DSGVO



Einverständniserklärung

*Für die Nutzung mit Werbung und Cookies: Wir, die Frankfurter Allgemeine Zeitung GmbH und unsere Partner, verarbeiten Daten (Informationen wie Cookies, Geräte-Kennungen, IP-Adresse) für unten näher beschriebene Zwecke. Es werden Informationen auf Ihrem Gerät gespeichert und abgerufen. Durch das Klicken des „Einverstanden"-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 Drittländern verarbeiten, in denen kein vergleichbares Datenschutzniveau vorherrscht (z.B. in den USA). In solchen Fällen ist es etwa möglich, dass Behörden dieser Drittländer auf die Daten Zugriff nehmen.

Informationspflicht nach DSGVO

Impressum (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

Datenschutzerklärung (Ausschnitt)

Inhaltsverzeichnis

1. Wir sind verantwortlich für Ihre Daten
2. Wie sicher sind Ihre Daten?
3. Unser Datenschutzbeauftragter
4. Was sind personenbezogene Daten?
5. Was sind Pflichtangaben oder Pflichtfelder?
6. Wofür werden Ihre Daten verarbeitet?

Copyright

Die Entscheidung, ob und wofür andere ein bestimmtes Werk verwenden dürfen, liegt beim Ersteller bzw. beim Autor. Grundsätzlich können Werke kostenlos oder kostenpflichtig zur Verfügung stehen.
Jedoch gilt: Auch wenn man Geld für eine Ressource bezahlt, heißt das nicht automatisch, dass man diese uneingeschränkt einsetzen darf. Der Schöpfer der Ressource kann entscheiden, ob und wofür sein Eigentum verwendet wird.

Public Domain

Was ist Public Domain?
Als Public Domain wird die urheberfreie Gemeinfreiheit von Dateien wie Musikstücken, Bildern oder aber ganze Software beschrieben.
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 den USA.
In Deutschland und den meisten anderen europäischen Staaten kann ein Urheber nicht komplett auf das Urheberrecht verzichten.

Fair Use

Oft stößt man im Internet auf den Ausdruck «Fair Use».
Wer denkt, dass damit gekennzeichnete Ressourcen für nicht kommerzielle Projekte verwendet werden können, der irrt sich.
Dateien, die unter der Kategorie «Fair Use» geführt werden, dürfen lediglich für bildende und künstlerische Zwecke eingesetzt werden.

Creative Commons (1)

Die von Laurence Lessing gegründete Organisation «Creative Commons» veröffentlichte sechs einfach verständliche Copyright Lizenzen – speziell für Online Medien. Hierbei handelt es sich um Bilder, Texte, Musikstücke oder Videoclips.

CC Attribution
Medien dürfen kostenlos kopiert und bearbeitet werden, sofern der Autor angegeben wird. Dies gilt auch für kommerzielle Projekte.

CC Attribution ShareAlike
Hierbei muss das Werk auch nach Veränderung unter derselben Lizenz weitergegeben werden.

CC Attribution NoDerivs
Das Werk darf nicht bearbeitet oder verändert werden.

CC Attribution NonCommercial
Das Werk darf nicht für kommerzielle Zwecke verwendet werden.

CC Attribution NonCommercial - ShareAlike
Das Werk darf nicht für kommerzielle Zwecke verwendet werden und lediglich unter gleichen Bedingungen weitergegeben werden.

CC Attribution NonCommercial - NoDerivs
Es ist verboten, das Werk zu bearbeiten und für kommerzielle Zwecke zu verwenden.

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 vom «Kleingedruckten». Die (wirtschaftlich stärkeren) Anbieter wollen damit die Verträge mit ihren (privaten) Kunden vereinheitlichen und rationell gestalten.

Damit AGB Bestandteil eines Vertrags werden, muss der Kunde sie bei Vertragsabschluss zur Kenntnis nehmen können. Der Anbieter muss sie also übergeben oder in geeigneter Form auf sie hinweisen, indem er sie zum Beispiel in seinen Geschäftsräumen unübersehbar 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.

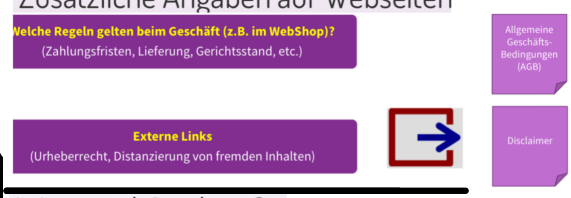
In den AGB sind die gegenseitigen Rechte und Pflichten der Vertragsparteien festgehalten. Da in der Schweiz Vertragsfreiheit besteht, haben AGB sehr oft Vorrang vor gesetzlichen Bestimmungen. Das kann dazu führen, dass Kundinnen und Kunden beim Akzeptieren von AGB auf Rechte, die ihnen das Gesetz zugestehen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



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 personenbezogenen 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 Nutzungsvorgang 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.