DSGVO
Datenschutz-Grundverordnung

Referent:
Bodo Wetzel
iota systems GmbH, 5400 Baden
www.iota.ch

DSGVO

- DEUTSCH: **DSGVO**
  - Datenschutz-Grundverordnung (88 Seiten)
- ENGLISH: **GDPR**
  - General Data Protection Regulation
- Gilt seit 25.05.2018
- https://dejure.org/gesetze/DSGVO

Grundrecht in der EU

- Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten

Agenda

- **Teil 1: Theorie und Grundlagen**
  - Räumlicher Anwendungsbereich
  - Umfang
  - Begriffe
  - Bedingungen
  - Rechtmässigkeit
  - Rechte
  - Pflichten
  - Sanktionen
- Teil 2: Konkrete Praxisbeispiele

Sind Schweizer Unternehmen überhaupt betroffen?

Artikel 3 Räumlicher Anwendungsbereich

(2) DSGVO ... findet Anwendung auf ... Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht

- a) betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;

Sind Schweizer Unternehmen überhaupt betroffen?

- Alle Organisationen, privat oder öffentlich, die Daten über europäische Bürger sammeln oder verwenden, sind von GDPR betroffen - auch Unternehmen in der Schweiz
- Typische Indikatoren:
  - Referenzkunden aus der EU
  - Angabe von Preisen in EUR

Was umfasst der Datenschutz?

Was umfasst der Datenschutz?

- Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei
  - der Verarbeitung personenbezogener Daten
  - und zum freien Verkehr solcher Daten

Artikel 4 Begriffsbestimmungen

- "Personenbezogene Daten" sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen
- Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt identifiziert werden kann
- Insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung

Artikel 4 Begriffsbestimmungen

"Verarbeitung" umfasst jeden ... ausgeführten Vorgang ... 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;

Artikel 4 Begriffsbestimmungen

- "Profiling" ist jede Art ..., die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte ... **zu bewerten**
- Insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu **analysieren** oder **vorherzusagen**

Gibt es weitere Bedingungen?

Artikel 5
Grundsätze

(1) **Personenbezogene Daten müssen**

a) auf rechtmässige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Mass beschränkt sein;

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist;

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet

Artikel 6
Rechtmässigkeit

!

Die **Verarbeitung ist nur rechtmässig**, wenn **mindestens eine** der nachstehenden Bedingungen erfüllt ist:

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist

c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen zu schützen;

e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt

f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen

Artikel 7
Bedingungen für die Einwilligung

(1) Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person eingewilligt hat.

(2) Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erfolgen.

(3) Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmässigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.

Artikel 4
Begriffsbestimmungen

"Einwilligung" der betroffenen Person:

Jede

- freiwillig
- für den bestimmten Fall,
- in informierter Weise und
- unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist

Welche Rechte haben die Besitzer von Personendaten?

Welche Rechte haben die Besitzer von Personendaten?

- Informationsrecht (Artikel 13)
- Auskunftsrecht (Artikel 14)
- Weitere ...

Artikel 13 Informationspflicht

(1) Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters
b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten (Data Protection Officer, DPO)
c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung

Artikel 13 Informationspflicht

(2) Zusätzlich ... stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:

a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
b) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
c) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
d) ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und

Artikel 14 Auskunftsrecht

(1) Die betroffene Person hat das Recht auf Auskunft über die personenbezogenen Daten und auf folgende Informationen:

a) die Verarbeitungszwecke
b) die Kategorien personenbezogener Daten, die verarbeitet werden
c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen
d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer
e) Etc.

Artikel 14 Auskunftsrecht

- Schriftlich
- Elektronisch (gängiges Format, z.B. PDF)
- Mündlich (Identität der betroffenen Person jedoch in anderer Form nachgewiesen werden)
- Nach Möglichkeit Fernzugang zu einem sicheren System bereitstellen, der der betroffenen Person direkten Zugang zu ihren personenbezogenen Daten ermöglichen würde.
- Angemessene Sicherheitsanforderungen eingehalten
- Innerhalb eines Monats (zwei Monate, wenn komplex)
- Kostenlos, in angemessenen Abständen (Art. 12 Abs. 5 DSGVO)

Weitere…

- Recht auf Berichtigung
- Recht auf Löschung (Recht auf Vergessen)
- Recht auf Beschwerde bei der Aufsichtsbehörde
- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit
- Widerspruchsrecht

Artikel 32
Sicherheit der Verarbeitung 1/2

(1) Der Verantwortliche und der Auftragsverarbeiter treffen geeignete technische und organisatorische Massnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten

Unter Berücksichtigung

- des Stands der Technik
- der Implementierungskosten
- der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung
- der unterschiedlichen Eintrittswahrscheinlichkeit
- der Schwere des Risikos

für die Rechte und Freiheiten natürlicher Personen

Artikel 32
Sicherheit der Verarbeitung 2/2

Diese Massnahmen schliessen unter anderem Folgendes ein:

- a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten
- b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen
- c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
- d) ein Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Wie ist bei Datenschutzverletzung vorzugehen?

Artikel 33
Meldepflicht an Aufsichtsbehörde

- (1) Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäss Artikel 51 zuständigen Aufsichtsbehörde
- Es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.
- Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

Meldepflicht an Datenbesitzer

- Sicherheitslücken müssen den Besitzern der Daten bekanntgegeben werden

Wie wird Nicht-Konformität sanktioniert?

- In Abhängigkeit des Engagement und der Schwere der Nicht-Konformität
  - Verwarnung
  - Bussen in Höhe von 4% des weltweiten Jahresumsatzes oder 20 Mio. EUR
  - Gefängnis

Agenda

- Teil 1: Theorie und Grundlagen ☑
- **Teil 2: Konkrete Praxisbeispiele**
  - Datenschutzbeauftragter
  - Verzeichnis der Verarbeitungstätigkeiten
  - Prozesshandbuch
  - Datenschutz-Folgeabschätzung
  - Auftragsdatenverarbeitung
  - Website

Datenschutzbeauftragter

Data Protection Officer, DPO

- Wenn mindestens zehn Personen (z.B. Sachbearbeiter, Rezeptionist, Sekretärin etc.) ständig mit der Verarbeitung von personenbezogenen Daten zu tun haben oder
- die Verarbeitung besonders risikoreich ist oder
- es sich bei dem Unternehmen um Adresshändler oder Auskunfteien handelt

Verzeichnis der Verarbeitungstätigkeiten

- Lohnabrechnung (z.B. durch Steuerberater oder intern)
- Personalverwaltung
- Betrieb der Firmenwebseite (auch über externe Hosting-Dienstleister)
- Kundenverwaltung
- Auftragsverwaltung
- IT-Support (extern)
- Auswertung von Kundendaten
- Zahlungsabwicklung bei Kunden
- Werbemassnahmen zur Kundengewinnung und -bindung

Verzeichnis der Verarbeitungstätigkeiten

Verantwortlich	Geschäftsführer XYZ, Adresse, Telefon, E-Mail
Zweck	Erbringung von Dienstleistungen, Versand von Produkten
Betroffene	Kunden der Firma XY / Bewerber bei der Firma XY
Wer kann auf die Daten zugreifen?	Alle Mitarbeiter der Firma XY
Datenkategorie	Bestellungen, Produkte, Dienstleistungen
Übermittlung an Drittstaaten	Nein
Löschfrist	Bei Widerruf des Betroffenen
Rechtsgrundlage	DSGVO Art. 6 (Rechtmässigkeit) Abs. 1b (Erfüllung eines Vertrages)
Einwilligung des Betroffenen	Jeder Kunde wird auf die Erfassung der Daten durch die Mitarbeiter mündlich hingewiesen und informiert, dass er diese Daten jederzeit einsehen und löschen lassen kann.

Prozesshandbuch

- Strikten Prozess- und Ablaufplan ausarbeiten
  - Internes Vorgehen bei einer Datenschutzverletzung
  - Bewertung im Hinblick auf bestehende Risiken
  - Kommunikation zwischen einzelnen Abteilungen
  - Hierbei muss darauf geachtet werden, dass wirklich alle Schutzverletzung zur Kenntnis des Verantwortlichen gelangen, damit dieser die erforderlichen Schritte einleiten kann
  - Nur 72 Stunden Zeit, um eine Datenschutzverletzung an die zuständige Aufsichtsbehörde zu melden

Prozesshandbuch

Verfahren zur

- zeitnahen Bearbeitung von Anfragen (Recht auf Auskunft, Berichtigung, Löschung, Datenübertragbarkeit, Widerspruch etc.)
- Zuordnung von Daten zu den sie betreffenden Personen,
- fristgerechten Löschung der Daten
- Identifikation und Klassifizierung von gespeicherten Daten und Orten im Sinne einer strukturierten Datenhaltung (z.B. in CRM, Akten oder mobile Devices etc.)

Datenschutzfolgeabschätzung

- Immer, wenn eine bestimmte Form der Verarbeitung, etwa aufgrund der Art, des Umfangs, der Umstände und der Zwecke, voraussichtlich (muss nicht gesichert sein) ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, müssen Sie eine Folgenabschätzung durchführen
- Achtung:
  Müssen Sie eine Datenschutz-Folgenabschätzung durchführen, so besteht gleichzeitig die Pflicht zur Bestellung eines Datenschutzbeauftragten, der Sie dabei wiederum unterstützen kann

Datenschutzfolgeabschätzung

- Denkbare Fälle, in denen eine Abschätzung erforderlich ist, sind beispielsweise:
  - Videoüberwachungsmassnahmen, insb. bei intelligenten und vernetzten Systemen
  - (Biometrische) Zugangssysteme
  - CRM-Software (inkl. Profiling-Funktionen)
  - Scorewertberechnungen und Persönlichkeitstests
  - Sicherheitsüberprüfungen (Betreibungsauskunft, Strafregisterauszug)
  - Monitoring-Systeme, etwa zur Überwachung von Mitarbeitern, etwa bei der Internetnutzung

Datenschutzfolgeabschätzung

Die Folgenabschätzung enthält zumindest Folgendes:

1. Systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschliesslich der von dem Verantwortlichen verfolgten berechtigten Interessen;
2. Bewertung der Notwendigkeit und Verhältnismässigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
3. Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäss Absatz 1
4. Zur Bewältigung der Risiken geplante Abhilfemassnahmen, einschliesslich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird

Auftragsdatenverarbeitung

- Prüfen Sie, ob für alle Datenverarbeitungen, die andere für Ihr Unternehmen im Auftrag und auf Ihre Weisung hin erbringen (z.B. Webhosting, Cloud-Services, Call-Center, Steuerberater, Werbeagentur), ein wirksamer Auftragsverarbeitungsvertrag geschlossen wurde und entsprechende Sicherheitsmassnahmen und sonstige Pflichtinhalte gemäss Art. 28 DSGVO enthalten sind.
- Fungieren Sie selbst als Auftragsverarbeiter? Dann beachten Sie die neuen Pflichten besonders, z.B. die Pflicht, ebenfalls ein Verarbeitungsverzeichnis über alle im Auftrag Ihrer Kunden verarbeiteten Daten zu führen.

Typische Fälle einer Auftragsverarbeitung

- Externe Lohn- oder Gehaltsabrechnung
- Newsletterversand durch eine Marketingagentur
- Nutzung von Cloud-Diensten zur Personal- und Kundenverwaltung
- Datenträgerentsorgung, Aktenvernichtung
- Lettershops, die in Ihrem Auftrag Werbung an Kunden versenden
- Webanalyse- und Trackings-Dienste wie Google Analytics
- Kunden-Helpdesks
- Ausgelagerte Rechenzentren
- Callcenter, die Kundendaten ohne wesentliche eigenen Entscheidungsspielräume verarbeiten
- Dienste, die Daten erfassen, konvertieren, Dokumente einscannen
- Auslagerung der Backup-Sicherheitsspeicherung/Archivierungen

Keine Auftragsverarbeitung

- Finanzberater
- Steuerberater
- Unternehmensberater
- Rechtsanwalt
- Wirtschaftsprüfer
- Externer Betriebsarzt
- Inkassobüro
- Bankinstitut für den Geldtransfer
- Postdienst für den Brieftransport
- Installation und Wartung von Netzwerken, Hardware, Telefonanlagen
- Pflege von Software
- Programmentwicklungen und Tests

Website

Zeitkritische öffentlichkeitswirksame Prozesse als erstes anpassen und überarbeiten

- Ein besonderes Augenmerk sollten Unternehmen nun auf alle Handlungen legen, die von aussen sichtbar sind und damit Aussenwirkung entfalten (Priorisierung)
- Dies gilt etwa im Hinblick auf die Websites (einschliesslich Kontaktformular), Webtracking, Datenschutzerklärungen auf der Homepage und der Überarbeitung von Einwilligungserklärungen. Hier stehen u.a. die Informationspflichten (Art. 13/14 DSGVO) im Fokus.

8 Punkte für Ihre Website

1. Sorgen Sie dafür, dass Ihre Website verschlüsselt ist
2. Überarbeiten Sie Ihre Datenschutzerklärung
3. Überprüfen Sie alle Formulare auf Ihrer Website
4. Überprüfen Sie Social-Media-Plugins und eingebettete Videos
5. Überprüfen Sie Ihr Statistik-Tool
6. Informieren Sie über Cookies
7. Überprüfen Sie Ihren Newsletter
8. Prüfen Sie, ob Sie mit Ihrem Webhoster einen Vertrag zur Auftragsverarbeitung schliessen müssen

1. Verschlüsselung

- Dies gilt in jedem Fall dort, wo es um Kontaktformulare oder Newsletter-Anmeldungen geht
- Verschlüsselte Seiten erkennt man daran, dass die URL mit https anfängt. Viele Browser zeigen dann ein Schloss vor der URL an oder das Wort "sicher"
- Mit Hilfe eines SSL-Zertifikats
- Kostenlose Zertifikate gibt es bei Let's Encrypt (https://letsencrypt.org)
- Übrigens: Nicht nur die DSGVO fordert verschlüsselte Internetseiten – auch in den Google-Suchergebnissen werden verschlüsselte Seiten bevorzugt angezeigt

2. Datenschutzerklärung

- Eine Datenschutzerklärung muss immer dann auf einer Internetseite vorhanden sein, wenn beim Besuch der Seite personenbezogene Daten erfasst und verarbeitet werden.
- Sie muss über Art, Umfang und Zweck der Erhebung und Verwendung von personenbezogenen Daten informieren.
- Darunter fallen neben der Erfassung von IP-Adressen und Personendaten insbesondere Hinweise
  - zum Umgang mit Social Plugins (zum Beispiel der Facebook „Like"-Button)
  - zum Umgang mit Kontaktformularen
  - zur Nutzung von Cookies
  - zum Einsatz von Analyse-Tools (wie etracker oder Google Analytics)
  - zu Targeting- und Zielgruppenoptimierungstools

2. Datenschutzerklärung - MUSS

- Kontaktdaten des Unternehmens bzw. des Verantwortlichen, der über die Verarbeitung von personenbezogenen Daten entscheidet (DPO)
- Alle Zwecke, zu denen personenbezogene Daten verarbeitet werden
- Rechtsgrundlagen für die Datenverarbeitung
  - Die zentrale Rechtsgrundlage, die die Erhebung und Verarbeitung personenbezogener Daten in bestimmten Fällen erlaubt, findet sich in Art. 6 der DSGVO
  - https://dejure.org/gesetze/DSGVO/6.html
- Speicherdauer der Daten
- Rechte der Betroffenen -> siehe nächste Folie

2. Datenschutzerklärung -> Nutzerrechte

- Nutzer müssen sehr umfassend über ihre Rechte informiert werden. Zu den **Nutzerrechten** zählen:
  - **Widerspruchsrecht/ Widerrufsrecht:** Beim Widerspruchsrecht gilt die Besonderheit, dass die Information darüber getrennt von den anderen Informationen erfolgen muss.
  - **Recht auf Auskunft:** Auf Nachfrage muss man Nutzern eine umfassende Auskunft über die Daten, die man von ihnen gespeichert hat, geben.
  - das **Recht, dass ihre Daten berichtigt oder gelöscht werden** oder die Verarbeitung eingeschränkt wird.
  - **Beschwerderecht bei einer Aufsichtsbehörde:** In Bezug auf das Beschwerderecht nach Art. 77 DSGVO ist es ausreichend, dass der Betroffene über das Recht als solches informiert wird. Es ist nicht nötig, die zuständige Datenschutzbehörde zu nennen.
  - **Recht auf Datenübertragbarkeit:** Dies bedeutet, dass beispielsweise Profile von einem Dienst auf den anderen übertragen werden, das ist vor allem auf soziale Netzwerke gemünzt.

2. Datenschutzerklärung – ggf.

- E-Mail-Adresse des Datenschutzbeauftragten
- Ihre berechtigte Interessen, die Sie mit der Datenverarbeitung verfolgen
- Dritte, an die die erhobenen personenbezogenen Daten übermittelt werden
- Ihre Absicht, die Daten ins Nicht-EU-Ausland zu übertragen (In diesem Fall müssen Sie erwähnen, ob es mit dem Zielland ein Datenschutzabkommen gibt oder nicht)
- Ob der Nutzer verpflichtet ist, seine Daten anzugeben und welche Folgen es hat, wenn er das nicht tun möchte
- Wenn eine automatisierte Entscheidungsfindung (zum Beispiel eine automatische Bonitätsprüfung im Hintergrund) besteht, müssen Sie das angeben

3. Formulare

- Kann man auf Ihrer Website einen Termin vereinbaren?
- Oder sich für einen Newsletter anmelden?
- Oder Ihnen über ein Formular eine Nachricht schreiben?

- Sie dürfen in ihren Formularen nur die personenbezogenen Daten erheben, die Sie tatsächlich brauchen, um eine Anfrage zu beantworten
- Für eine Newsletter-Anmeldung benötigt man beispielsweise grundsätzlich nur die E-Mail-Adresse, nicht aber den Vor- und Zunamen. Daher dürfen die Felder für den Vor- und den Nachnamen keine Pflichtfelder sein.
- Pflichtfelder in Formularen – in diesem Fall nur das Feld für die E-Mail-Adresse – müssen gekennzeichnet sein
- Wenn Sie noch weitere Daten erheben wollen, dann muss für den Nutzer klar sein, dass diese Angaben freiwillig sind.

3. Formulare

Beispielformulierung auf Web-Formular:

"Wir verarbeiten Ihre Vertragsdaten (z.B. in Anspruch genommene Leistungen, Namen von Kontaktpersonen, Zahlungsinformationen), um unsere vertraglichen Verpflichtungen und Serviceleistungen gemäss Art. 6 Abs. 1b DSGVO zu erfüllen. Die in Onlineformularen als verpflichtend gekennzeichneten Angaben sind für den Vertragsschluss erforderlich."

4. Social Media/Video

- Die Social-Media-Plugins, die Facebook und Co. zur Verfügung stellen, sammeln vom Websitenutzer unbemerkt personenbezogene Daten und können so detaillierte Persönlichkeitsprofile erstellen
- Dasselbe gilt, wenn Sie Videos, beispielsweise von Youtube oder Vimeo, auf Ihrer Seite einbetten
- Haben Sie zum Beispiel Youtube-Videos auf Ihrer Seite eingebaut, dann übertragen Sie automatisch Daten Ihrer Websitebesucher an Youtube (und damit Google) – unabhängig davon, ob der Nutzer das Video anklickt oder nicht

4. Social Media Plug-Ins

DSGVO-Konformität erreichen

- Eine Möglichkeit ist, zum Beispiel den Facebook-Like-Button einfach zu entfernen
- Wer darauf nicht verzichten will, kann auf Lösungen wie Shariff (https://github.com/heiseonline/shariff) zurückgreifen.
  Hierbei können Besucher erst nach Aufruf der Webseite frei entscheiden, ob ihre Daten durch die Plug-ins an die Sozialen Netzwerke übertragen werden sollen oder nicht.

4. Videos

- Wenn Sie Youtube-Videos auf Ihrer Seite einbetten, dann verwenden Sie dafür den "erweiterten Datenschutzmodus"
  Sie finden ihn unter
  "Teilen" > "Einbetten" > "Mehr anzeigen"
- Für Vimeo gibt es momentan noch keine DSGVO-konforme Lösung

5. Statistik-Tool (Google Analytics)

- Google Analytics sammelt IP-Adresse, welche so gekürzt (anonymisiert) werden müssen, dass kein Personenbezug mehr möglich ist
- Webadministrator: "anonymizeIP"-Befehl in HTML-Source
- Zudem müssen Sie mit Google einen Vertrag zur Auftragsverarbeitung schliessen und in der Datenschutzerklärung darauf hinweisen, dass Sie das Statistik-Tool verwenden
- Link zu den Google Analytics Nutzungs- und Datenschutzbestimmungen zur Verfügung stellen
- Widerspruchsmöglichkeit (Opt-out) integrieren
  - Mit einem Klick in den Datenschutzerklärungen kann ein Nutzer dafür sorgen, dass seine Daten nicht mehr an Google weitergegeben werden
  - Wie man diese Opt-out-Funktion integriert, ist hier bei Google beschrieben

6. Cookies

- Kleine Dateien, die Daten lokal auf dem Gerät speichern
- Sie dienen dazu, den Nutzer wiederzuerkennen und ihm das Surfen auf der Website zu erleichtern
- Rechtliche Lage nach Inkrafttreten der DSGVO noch unklar
- Um Abmahnungen zu vermeiden, sollte man von den Websitenutzern beim ersten Aufruf der Seite in der so genannten Cookie-Warnung die Einwilligung einholen:
  - *„Um unsere Webseite für Sie optimal zu gestalten und fortlaufend verbessern zu können, verwenden wir Cookies. Durch die weitere Nutzung der Webseite stimmen Sie der Verwendung von Cookies zu. Weitere Informationen zu Cookies erhalten Sie in unserer Datenschutzerklärung.*"
- Die DSGVO verlangt, dass in Datenschutzerklärung die Rechtsgrundlagen für das Verwenden von Cookies genannt werden
- Ausserdem muss ein Hinweis für die Nutzer in die Datenschutzerklärung, wie sie das Setzen von Cookies verhindern können

7. Newsletter überprüfen

- Newsletter-Dienste MailChimp, CleverReach und Newsletter2Go
  - Vertrag zur Auftragsverarbeitung mit Dienstleister schliessen
- Anmeldeformular überarbeiten
  - Zweck des Newsletters
  - Welche Informationen Abonnenten erhalten
  - Als Pflichtfeld lediglich die E-Mail-Adresse
  - Link zur Datenschutzerklärung mit Hinweis, dass ausgewertet wird, wie viele Benutzer einen Link in einem Newsletter anklicken (Begründung: Verbesserung der Inhalte)
- Deutlicher Hinweis auf Widerrufsrecht der Anmeldung
  - Link zu Abmeldeformular (auf Anmeldung und in jedem Newsletter)

7. Newsletter überprüfen

- Double-Opt-In:
  - Damit nicht jemand gegen seinen Willen als Abonnent eingetragen wird und Sie die Einwilligung rechtssicher nachweisen können
  - Nutzer muss über einen personalisierten Bestätigungslink (sogenannte Check-Mail) nochmals bestätigen, dass er tatsächlich Inhaber dieses Postfachs ist

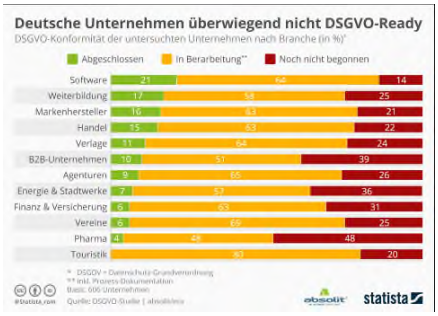
8. Vertrag mit Webhoster

- Der Webhoster (Provider) stellt Webseiten bereit und übernimmt den Betrieb von Webservern und die Netzwerkanbindung
- Ist mit solchen Dienstleistungen nur der Internet-Zugangsdienst ohne die Verarbeitung von personenbezogenen Daten verbunden, dann liegt keine Auftragsverarbeitung vor
- Übernehmen solche Webhoster allerdings auch Aufgaben, bei denen sie personenbezogene Daten verarbeiten, wie beispielsweise die E-Mail-Verwaltung oder die E-Mail-Archivierung, dann liegt eine Auftragsverarbeitung vor und Sie müssen einen Vertrag zur Auftragsverarbeitung schliessen

Agenda

- Teil 1: Theorie und Grundlagen ☑
- Teil 2: Konkrete Praxisbeispiele ☑

Aufgeschreckt? Sie sind nicht alleine!



Besten Dank für Ihre Aufmerksamkeit

Kontakt
Bodo Wetzel
iota systems GmbH
5400 Baden / 4014 Oberwil
www.iota.ch