Datenschutzrecht für WebShops

Die Daten-schutzgruppe

Die Daten-schutzgruppe

Rechtsanwältin
Mag. Birgit Noha, LLM
zertifizierte Datenschutzbeauftragte
Zieglergasse 1/18
A-1070 Wien
Tel: +43 (1) 522 27 29
Fax: +43 (1) / 5239001 – 91
Mail: office@laws.at
www.laws.at
Laws.at

Netzwerktechnik
Traub
Prof. Dr. Stephan Koren Straße 10
2700 Wiener Neustadt
Tel: +43 (2622) 90 8 14
Mail: office@traub.at
www.traub.at

Solutions Coach
Martin Jestl
Maygasse 4/8/1
A-1130 Wien
Tel: +43 (699) 1599 1058
Mail: master@wizzard.solutions
www.wizzard.solutions

Datenschutz neu

- *24.5.2016: Inkrafttreten der Datenschutz-Grundverordnung, 2 Jahre Umsetzungsfrist*
- *25.5.2018: Anwendbarkeit der DSGVO*
- *25.5.2018: Geltung des DSGVO-Begleitgesetzes („DSG“) in Österreich*

Grundlagen des Datenschutzrechts

- *Definitionen*
- *Datenschutzgrundsätze*
- *Rechtmäßigkeit der Datenverarbeitung und Rechenschaft im Webshop*
- *Erfüllung der vertraglichen Verpflichtung*
- *Einwilligung - Voraussetzungen*
- *Verfahrensverzeichnis für einen Webshop*
- *Datenübermittlung in unsichere Drittstaaten*
- *Informationspflicht im Webshop (data protection policy)*
- *Betroffenenrechte*
- *Was passiert mit Altbeständen an Daten?*
- *Data Breach*
- *TOMS im Webshop, insbesondere Privacy per Design & Default*
- *Strafen und Sanktionen*

Daten im WebShop

Wenn Sie (auf Ihrer Website) personenbezogene Daten verarbeiten (insbesondere Erheben, Erfassen, Speichern, Auslesen, Abfragen, Verwenden, Ändern, Abgleichen, Übermitteln, Bereitstellen, Verknüpfen) haben Sie die geltenden Datenschutzbestimmungen einzuhalten. Die IP-Adresse gilt als personenbezogenes Datum.

Wenn Sie einen Webshop betreiben, verarbeiten Sie jedenfalls personenbezogene Daten und haben daher die jeweils geltenden Datenschutzbestimmungen einzuhalten. Jede Datenverarbeitung hat den in der DSGVO normierten Grundsätzen zu entsprechen. Dazu gehört neben einem gerechtfertigten Zweck und dem Grundsatz der Datenminimierung (auch im Hinblick auf Speicherdauer) unter anderem die Rechtmäßigkeit der Datenverarbeitung.

Was ist Datenverarbeitung?

- *Erheben… Erfassen… Organisation… Ordnen… Speicherung… Anpassung… Veränderung… Auslesen… Abfragen… Verwendung… Offenlegung durch Übermittlung… Verbreitung… Bereitstellung… Abgleich… Verknüpfung… Einschränkung… Löschen… Vernichtung*
- *Eine sortierte Sammlung von Visitenkarten*
- *Abgelegte Mails sind Datenverarbeitung!*

Definitionen

- *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, zB Webshopbetreiber*
- *Betroffene Person: identifizierte oder identifizierbare Person, auf die sich Informationen beziehen*
- *Auftragsverarbeiter: eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet*

Personenbezogene Daten

„Kategorien“ von Daten (sensible Daten)

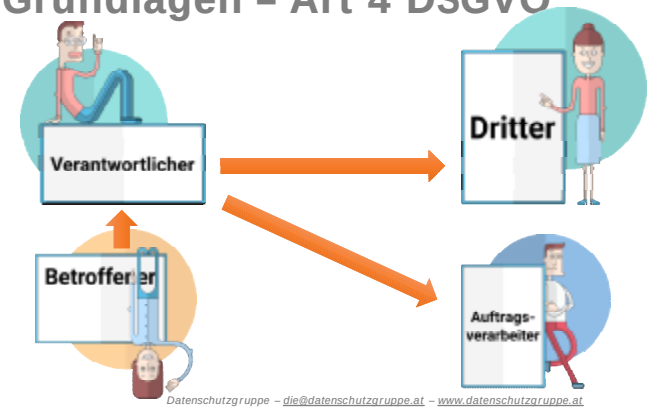
- **rassische/ethnische Herkunft**
- **politische Meinungen**
- **religiöse/weltanschaul. Überzeugungen**
- **Gewerkschaftszugehörigkeit**
- *genetische Daten*
- **biometrische Daten**
- **Gesundheitsdaten**
- **Daten zum Sexualleben**
- **sexuelle Orientierung**

=> GRUNDSATZ: Verbot der Verarbeitung !

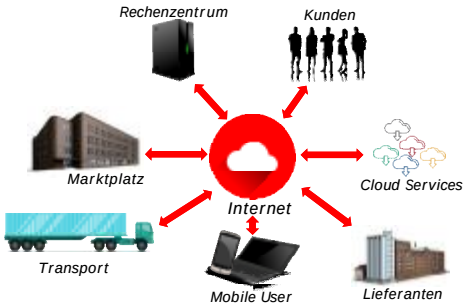
Ausnahme vom Verbot:

- **ausdrückliche Einwilligung**
- *Schutz lebenswichtiger Interessen*
- **offensichtlich selbst öffentlich gemacht**
- *Arbeitsrecht, Sozialrecht,*
- *Rechtsverfolgung/-verteidigung*
- **öffentliche Gesundheit**
- **im öffentlichen Interesse**:
- *Archivzwecke, wissenschaftliche*
- *o. historische Forschung, Statistik*
- **Fachpersonal, Berufsgeheimnis, Geheimhaltungspflichten**
- **FREIHEIT der Meinungsäußerung und Informationsfreiheit ??!**

Grundlagen – Art 4 DSGVO



Verarbeiter und Übertragung



Anwendungsbereich der DSGVO

Kann ich identifizieren/identifiziert werden

Datenschutz neu und insbesondere die Auswirkungen auf WebShops

Für Cookies und Online-Direktwerbung (z.B. E-Mail-Newsletter) wird es eine eigene Datenschutz-Verordnung elektronische Kommunikation – E-DSVO) geben. Bis dahin gelten die Bestimmungen des Telekommunikationsgesetzes (TKG).

- *Rechtsgrundlage für die Zulässigkeit der Verwendung*
- *Informationsplichten bei der Datenerhebung bzw –verwendung (Datenschutzerklärung)*
- *Privacy by design/privacy by default*
- *Rechte der Betroffenen, Datenportabilität*
- *Verträge mit Auftragsverarbeitern und Rechtmäßigkeit für Übermittlung in Drittstaaten*
- *Allenfalls Zustimmungserklärungen der Kunden*
- *Dokumentationspflicht*

Räumlicher Anwendungsbereich

- **Niederlassung in der EU**
  - *Unternehmen das die Daten verarbeitet („Verantwortlicher“)*
  - *Dienstleister („Auftragsverarbeiter“)*
  - *auch wenn Ort der Verarbeitung außerhalb der EU (zB Server in USA)*
- **Niederlassung außerhalb der EU**
  - **„Marktortprinzip“**
  - *Angebot (Waren, Dienstleistungen) => EU*
  - *Verhalten beobachten, analysieren => EU (zB Google-Analytics)*

Datenschutz ist ein Grundrecht und grundsätzlich verboten, außer .....

...Eine Datenverarbeitung ist also dann rechtmäßig, wenn (Art 6 DSGVO)

- *Erfüllung eines Vertrages? Notwendigkeit zur Vertragserfüllung oder vorvertraglicher Maßnahmen*
- *Einwilligung?*
- *Rechtliche Verpflichtung?*
  (z.B.: ASVG für AN-Daten)
- *Überwiegende berechtigte Interessen des Verantwortlichen?*
  (z.B.: Konzerninteressen)
- *Anonymisiert?*
- *Verwendung im lebenswichtigen Interesse des Betroffenen oder eines Dritten*
- *Wahrnehmung einer Aufgabe im öffentlichen Interesse*
- *Daten sind öffentlich*

Die rechtliche Basis einer Verarbeitung muss immer dokumentiert werden, damit sie bei einer Überprüfung Gültigkeit hat!!

Datenschutzgrundsätze (Art. 5)

Folgende Grundsätze gelten für jede Datenverarbeitung:

- *Rechtmäßigkeit, Fairness („Treu und Glauben") und Transparenz!*
- *Zweckbindung: Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke, nicht in mit diesen zwecken unvereinbarer Weise weiterverwenden!*
- *Datenminimierung: Nur soviel Datenverarbeitung, als zur Erreichung des Zwecks nötig!*
- *Richtigkeit: sachlich richtig, aktuell.*
- *Speicherbegrenzung: möglichst pseudonymisieren (Datensparsamkeit) oder Daten löschen, wenn keine Speicherpflichten (Archivierungs- oder Aufbewahrungspflichten) mehr vorhanden!*
- *Integrität und Vertraulichkeit: organisatorische und technische Schutzmaßnahmen*
- *Rechenschaftspflicht – man muss zu allen Rede und Antwort stehen können!*

Überwiegende Interessen des Verantwortlichen (Art 6 Abs 1 Z f DSGVO)

z.B.: zur Verhinderung von Betrug, zur Geltendmachung von Rechtsansprüchen des Verantwortlichen vor einer Behörde

Bisherige Judikatur DSBeh: übergeordnete Konzerninteressen argumentierbar (zB Konzerncontrolling, Konzernplanung, Matrixorganisation)

Überwiegende wirtschaftliche Interessen können nie die Verarbeitung von besonderen Kategorien von Daten iSd Art 9 rechtfertigen!

Gültige Einwilligung im WebShop (Art 7 DSGVO)

Definition (Art 4 Z 11 DSGVO):

„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

- *Freiwillig = ohne Zwang: ist bei eigenen Mitarbeitern typischer Weise nicht gegeben, da wirtschaftlich ungleich!*
- *Informiert = in voller Kenntnis der Sachlage*
- *Achtung auf Kopplungsverbot: Vertragsgegenstand und Werbezustimmung sind zu trennen!*

Informationspflicht im WebShop (Datenschutzerklärung)

Im Zusammenhang mit einem Internetauftritt werden "personenbezogene Daten" erhoben, d.h. festgehalten und gespeichert.

➡ *Pflicht zur Verwendung einer gesonderten Datenschutzerklärung*

Diese hat zu enthalten:

Gesonderte Datenschutzerklärung

- *Name und Kontaktdaten des für die Datenverarbeitung Verantwortlichen*
- *Zweck sowie Rechtsgrundlage für die Verarbeitung, ggf Angabe der berechtigten Interessen zur Datenverarbeitung wenn diese auf einer Interessenabwägung beruht*
- *Empfänger oder Kategorien von Empfängern*
- *Absicht, Daten an ein Drittland oder eine internationale Organisation zu übermitteln*
- *Speicherdauer, bzw Kriterien für die Festlegung der Dauer*
- *Hinweis auf das Auskunftsrecht, Berichtigungsrecht und Löschungsrecht oder Einschränkung der Verarbeitung sowie auf das Widerspruchsrecht und das Recht auf Datenübertragbarkeit*

Gesonderte Datenschutzerklärung

- *Hinweis auf das Widerrufsrecht, wenn die Daten durch Einwilligung erhoben wurden*
- *Hinweis auf ein allfälliges Beschwerderecht bei einer Aufsichtsbehörde*
- *Hinweis, wie weit die Datenbereitstellung gesetzlich oder vertraglich vorgeschrieben ist oder für den Vertragsabschluss erforderlich ist*
- *Hinweis, ob die betroffene Person verpflichtet ist, die Daten bereit zu stellen und welche möglichen Folgen die Nichtbereitstellung hätte*
- *Hinweis, ob die Daten zu einer automatisierten Entscheidungsfindung (einschließlich Profiling) verwendet werden und eine allgemein verständliche Darstellung der Entscheidungslogik sowie der Tragweite der Auswirkungen einer derartigen Verarbeitung*
- *Verwendung der Daten für einen anderen als den ursprünglichen Verwendungszweck => neue Informationspflicht*

Auch dann, wenn Daten nicht beim Betroffenen ermittelt werden

In diesem Fall zusätzlich Informationen übe die Herkunft der Daten und Datenarten

Spätestens binnen 1 Monat

Ausnahmen:

- *Information ist bereits bekannt*
- *Information ist unmöglich oder nur unter unverhältnismäßigem Aufwand möglich, dann öffentlich zur Verfügung stellen*
- *die Verarbeitung erfolgt aufgrund von Rechtsvorschriften*
- *Daten müssen vertraulich behandelt werden*

Konsequenzen

Strafen

- *bis zu € 20 Mio (bisher max. € 25.000,--)*
- *oder bis zu 4% des weltweiten Vorjahresums*

zivilrechtliche Ansprüche

- *Auskunft, Berichtigung, Einschränkung, Löschung, Mitteilung, Übertragbarkeit, Widerspruch*
- *Mitbewerber: Unterlassung nach UWG*

Strafbemessungskriterien

- *Art, Schwere und Dauer des Verstoßes*
- *Kategorien besonderer Daten*
- *Ergriffene Maßnahmen zur Schadensminderung*
- *Ausmaß der im Vorfeld ergriffenen technischen oder organisatorischen Datensicherheitsmaßnahmen*
- *Meldung des Verstoßes an die Aufsichtsbehörde*
- *Durch Verstoß erlangte finanzielle Vorteile*
- *Frühere Verstöße*

Altbestand

- *Wenn keine Zustimmung belegbar, ist sie nicht akzeptabel*
- **DSGVO, ErwG171 :** *„Beruhen die Verarbeitungen auf einer Einwilligung gemäß der Richtlinie 95/46/EG, so ist es nicht erforderlich, dass die betroffene Person erneut ihre Einwilligung dazu erteilt, wenn die Art der bereits erteilten Einwilligung den Bedingungen dieser Verordnung entspricht, so dass der Verantwortliche die Verarbeitung nach dem Zeitpunkt der Anwendung der vorliegenden Verordnung fortsetzen kann. Auf der Richtlinie 95/46/EG beruhende Entscheidungen bzw. Beschlüsse der Kommission und Genehmigungen der Aufsichtsbehörden bleiben in Kraft, bis sie geändert, ersetzt oder aufgehoben werden."*

alte Einwilligungen gelten, wenn

- *auf* **Grundlage der bisherigen Rechtslage gültig** *abgegeben und*
- *die* **Bedingungen der DSGVO** *erfüllen*

alte Vereinbarungen überprüfen

Datenübermittlung in Drittländer

Gleichgestellt mit EU:

- *EU, alle Mitgliedstaaten und EWR*

Angemessenheitsbeschluss der Kommission:

- *Schweiz, Guernsey, Jersey, Isle of Man, Färöer-Inseln, Argentinien, Andorra, Israel, Kanada, Uruguay, Neuseeland*
- *USA: nur „Privacy Shield" – zertifizierte Unternehmen (www.privacyshield.gov)*
- *Transfer mit Standardvertragsklauseln künftig genehmigungsfrei (aber nur wenn Klauseln nicht verändert werden)*
- *Verbindliche interne Vorschriften im Konzern (Binding Corporate Rules), wenn von der Datenschutzbehörde genehmigt*

Für Drittstaaten ist keine Genehmigung erforderlich, wenn zB

- *die Daten anonymisiert sind*
- *die ausdrückliche Einwilligung vorliegt, sofern über bestehende Risken informiert würde*
- *ein Vertrag zwischen Verantwortlichen und Betroffenen nicht anders als durch die Übermittlung der Daten ins Ausland erfüllt werden kann (Vertragserfüllung)*
- *die Übermittlung zum Abschluss oder zur Erfüllung eines im Interesse des Betroffenen geschlossenen Vertrages notwendig ist*
- *die Übermittlung zur Geltendmachung von Rechtsansprüchen erforderlich ist*

Auftragsdatenverarbeitung

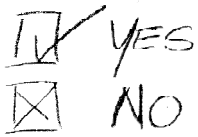
- *Auftragsverarbeiter muss ausreichende Gewähr für rechtmäßige und sichere Datenverarbeitung bieten*
- *(Nachweis mittels Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens möglich!)*
- *schriftlicher Vertrag Verantwortlicher – Auftragsverarbeiter*
- *mindestens Pflichten nach Art 28 DSGVO*

Gilt auch bei Cloud Computing, Transportdienstleister, Zahlungsdienstleister, MailChimp etc.

Auftragsdatenverarbeitung international

- *Möglich, sogar ohne Zustimmung, wenn für Vertragserfüllung notwendig*

Wenn nicht: Einwilligung der User einholen, oder Standardvertragsklauseln abschließen



Rechte des Betroffenen

- **Informationspflichten** *und* **Auskunftsrecht** *(ua auch über geplante Speicherdauer)*
- *Recht auf* **Berichtigung**
- *Recht auf* **Löschung** *und Recht auf „Vergessen werden"*
- *Recht auf* **Einschränkung** *der Verarbeitung*
- **Mitteilungspflicht** *bei Berichtigung, Löschung oder Einschränkung an alle Empfänger*
- *Recht auf* **Datenübertragbarkeit** *(Mitnahme von einem Anbieter zum nächsten)*
- **Widerspruchsrecht**
- *Beschwerdemöglichkeiten bei Aufsichtsbehörde*

Reaktionszeit auf Anfragen: Frist: 1 Monat + *max. 2 Monate*

Auskunftsrecht (Art 15 DSGVO)

Verantwortliche müssen bekannt geben, ob Daten über eine bestimme Person verarbeitet werden. Bei Verarbeitung:

- *Verarbeitungszweck*
- *Kategorien personenbezogener Daten*
- *Empfänger/Kategorien von Empfängern, speziell bei Empfängern in Drittstaaten: Informationen über die geeigneten Garantien (zB (Standard)vertragsklauseln, BCR, etc im Zusammenhang mit der Übermittlug*
- *Speicherdauer, ggf Kriterien für deren Festlegung*
- *das Bestehen von Berichtigungs- Löschungs- Widerspruchsrechten oder auf Einschränkung der Verarbeitung personenbezogener Daten, das Bestehen eines Beschwerderechts bei eine Aufsichtsbehörde*
- *Auskunft muss unentgeltlich sein, außer offenkundig oder exzessiv => angemessenes Entgelt*

Recht auf Datenübertragbarkeit (Art 20 GSGVO?

- *Recht betroffener Personen, zur Verfügung gestellte Daten in maschinenlesbarer Art zu erhalten und an einen anderen Verantwortlichen zu übertragen, wenn die Verarbeitung aufgrund einer Einwilligung oder eines Vertrages erfolgt*
- *Wenn technisch möglich, sollen die Daten direkt zwischen Verantwortlichen übertragen werden*
- *Ausnahmen: Verarbeitung für die Wahrnehmung einer Aufgabe des öffentlichen Interesses oder*
- *Rechte und Freiheiten anderer würden verletzt*

Organisatorische Umsetzung im Webshop

Planung und Organisation

- *Prozess Analyse*
  Wissen Sie was in Ihrer Firma los ist?
- *Erhebung der Informationen bezüglich Personen bezogener Daten*
- *Entwicklung effizienter Strategien*

Technische Umsetzung im Webshop

Erreichen eines Grundschutzes im Unternehmen durch Technikeinsatz

- *Applications Firewalls*
- *Verschlüsselung*
- *2-Faktor Authentifizierung*
- *Versperrbare Türen/Kästen/Server/etc...*
- *usw ...*

Für mehr Informationen sind wir gerne für Sie da!

Die Daten-schutzgruppe