Datenschutz im Internet - Recht auf Vergessen

Diplomarbeit

zur Erlangung des akademischen Grades

Magister der Rechtswissenschaften

im Diplomstudium

Rechtswissenschaften
Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass ich die vorliegende Diplomarbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt bzw die wörtlich oder sinngemäß entnommenen Stellen als solche kenntlich gemacht habe.

Die vorliegende Diplomarbeit ist mit dem elektronisch übermittelten Textdokument identisch.

Naarn, am 08.01.2016

Ing. Michael Furtlehner
DANKSAGUNG

Zu Beginn darf ich mich bei all jenen bedanken, die mich zu diesem berufsbegleitenden Studium motiviert und mich dabei immer unterstützt haben.


Besonderer Dank gilt meiner Frau Gudrun, nicht nur für die Korrekturvorschläge in dieser Arbeit, sondern auch für das aufgebrachte Verständnis und die ständige Motivation und Unterstützung während der gesamten Studiendauer.
# Inhaltsverzeichnis

## 1 Einleitung

1.1 Begriffsbestimmungen
1.1.1 Personenbezogene Daten
1.1.2 Betroffener
1.1.3 Auftraggeber
1.1.4 Dienstleister
1.1.5 Datenverarbeitung
1.2 Entwicklung des Datenschutzes in Österreich

## 2 Rechtsgrundlagen

2.1 EU-Datenschutz-Richtlinie 95/46/EG
2.2 Datenschutzgesetz 2000 (DSG)
2.2.1 Grundrecht auf Datenschutz
2.2.2 DVR und Meldepflicht
2.2.3 Rechtsschutz
2.3 E-Commerce Gesetz (ECG)
2.3.1 Ausschluss der Verantwortlichkeit bei Suchmaschinen (§ 14 ECG)
2.3.2 Herkunftslandprinzip und seine Ausnahmen (§§ 20 ff ECG)
2.4 Künftiges EU-Datenschutzrecht (DSGVO)

## 3 Datenschutz im Internet

3.1 Datenschutzbehörde
3.2 Datenschutzbeauftragter
3.2.1 Kompetenzen und Fähigkeiten des bDSB
3.2.2 Aufgabengebiete des bDSB
3.3 Vorratsdatenspeicherung
3.4 Systemanbieterhaftung
3.4.1 Access-Provider
3.4.2 Hosting-Provider
3.5 Haftung für Links auf fremde Websites
3.6 Haftungsausschluss für Suchmaschinen
# Inhaltsverzeichnis

4 EuGH-Urteil C-131/12

4.1 Sachverhalt

4.2 Schlussanträge des Generalanwalts

4.3 Kritische Betrachtung des Urteils

4.4 Auswirkungen für den Suchmaschinenbetreiber

5 Recht auf Löschung der Daten

5.1 Lösung aus den Google-Suchergebnissen

5.1.1 Voraussetzungen und Lösungsantrag

5.1.2 Lösung der Daten aus Sicht von Google

5.2 Lösung im Unternehmensbereich

5.2.1 Urheberrechtliche Aspekte von Inline-Links und Framing

5.2.2 Wettbewerbsrechtlicher Schutz von Kennzeichen, Marken und Domains

5.2.3 Mitarbeiterdaten

5.3 Lösung im Privatbereich

6 Konklusion
# Abkürzungsverzeichnis

<table>
<thead>
<tr>
<th>Abkürzung</th>
<th>Deutscher Ausdruck</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABGB</td>
<td>Allgemeines bürgerliches Gesetzbuch JGS 1811/946</td>
</tr>
<tr>
<td>Abs</td>
<td>Absatz</td>
</tr>
<tr>
<td>AEPD</td>
<td>Agencia Española de Protección de Datos</td>
</tr>
<tr>
<td>ArbVG</td>
<td>Arbeitsverfassungsgesetz BGBl 1974/22</td>
</tr>
<tr>
<td>Art</td>
<td>Artikel</td>
</tr>
<tr>
<td>ASvV</td>
<td>Ausschuss der Ständigen Vertreter</td>
</tr>
<tr>
<td>bDSB</td>
<td>betrieblicher Datenschutzbeauftragter</td>
</tr>
<tr>
<td>BGBl</td>
<td>Bundesgesetzblatt</td>
</tr>
<tr>
<td>B-VG</td>
<td>Bundes-Verfassungsgesetz BGBl 1930/1</td>
</tr>
<tr>
<td>BVwG</td>
<td>Bundesverwaltungsgericht</td>
</tr>
<tr>
<td>BVwGG</td>
<td>Bundesverwaltungsgerichtsgesetz BGBl I 2013/10</td>
</tr>
<tr>
<td>bzw</td>
<td>beziehungsweise</td>
</tr>
<tr>
<td>ccTLD</td>
<td>Country-Code TopLevel Domain</td>
</tr>
<tr>
<td>dh</td>
<td>das heißt</td>
</tr>
<tr>
<td>DSB</td>
<td>Datenschutzbehörde</td>
</tr>
<tr>
<td>DSG 2000</td>
<td>Datenschutzgesetz 2000 BGBl 165/1999</td>
</tr>
<tr>
<td>DSGVO</td>
<td>EU-Datenschutz-Grundverordnung</td>
</tr>
<tr>
<td>DVR</td>
<td>Datenverarbeitungsregister, Datenverarbeitungsregister</td>
</tr>
<tr>
<td>E</td>
<td>Entscheidung</td>
</tr>
<tr>
<td>ECG</td>
<td>E-Commerce-Gesetz BGBl I 2001/152</td>
</tr>
<tr>
<td>E-GovG</td>
<td>E-Government-Gesetz BGBl I 2004/10</td>
</tr>
<tr>
<td>etc</td>
<td>et cetera</td>
</tr>
<tr>
<td>Abkürzung</td>
<td>Erklärung</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------</td>
</tr>
<tr>
<td>EU</td>
<td>Europäische Union</td>
</tr>
<tr>
<td>EuGH</td>
<td>Europäischer Gerichtshof, Gerichtshof der Europäischen Union</td>
</tr>
<tr>
<td>gem</td>
<td>gemäß</td>
</tr>
<tr>
<td>GewO</td>
<td>Gewerbeordnung 1994 BGBI 1994/194</td>
</tr>
<tr>
<td>ggf</td>
<td>gegebenenfalls</td>
</tr>
<tr>
<td>grds</td>
<td>grundsätzlich</td>
</tr>
<tr>
<td>gTLD</td>
<td>Generic Top Level Domain</td>
</tr>
<tr>
<td>hA</td>
<td>herrschende Ansicht</td>
</tr>
<tr>
<td>ICANN</td>
<td>Internet Corporation for Assigned Names and Numbers</td>
</tr>
<tr>
<td>idF</td>
<td>in der Fassung</td>
</tr>
<tr>
<td>idgF</td>
<td>in der geltenden Fassung</td>
</tr>
<tr>
<td>idR</td>
<td>in der Regel</td>
</tr>
<tr>
<td>ieS</td>
<td>im engeren Sinn</td>
</tr>
<tr>
<td>iHv</td>
<td>in Höhe von</td>
</tr>
<tr>
<td>iSd</td>
<td>im Sinne des, der</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>IT</td>
<td>Informationstechnologie</td>
</tr>
<tr>
<td>iVm</td>
<td>in Verbindung mit</td>
</tr>
<tr>
<td>LG</td>
<td>Landesgericht</td>
</tr>
<tr>
<td>Mio</td>
<td>Million, -en</td>
</tr>
<tr>
<td>Mrd</td>
<td>Milliarde, -n</td>
</tr>
<tr>
<td>MRK</td>
<td>(Europäische) Menschenrechtskonvention BGBI 1958/210</td>
</tr>
<tr>
<td>NSA</td>
<td>National Security Agency</td>
</tr>
<tr>
<td>og</td>
<td>oben genannte, -n</td>
</tr>
<tr>
<td>OGH</td>
<td>Oberster Gerichtshof</td>
</tr>
<tr>
<td>Pkt</td>
<td>Punkt</td>
</tr>
<tr>
<td>RL</td>
<td>Richtlinie</td>
</tr>
<tr>
<td>sog</td>
<td>so genannt, -e, -er, -es</td>
</tr>
<tr>
<td>SPG</td>
<td>Sicherheitspolizeigesetz BGBI 1991/566</td>
</tr>
<tr>
<td>ua</td>
<td>unter anderem</td>
</tr>
<tr>
<td>UDRP</td>
<td>Uniform Domain-Name Dispute-Resolution Policy</td>
</tr>
<tr>
<td>Abkürzung</td>
<td>Bedeutung</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>UrhG</td>
<td>Urheberrechtsgesetz BGBl 1936/111</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
<tr>
<td>uU</td>
<td>unter Umständen</td>
</tr>
<tr>
<td>UWG</td>
<td>Bundesgesetz gegen den unlauteren Wettbewerb 1984 BGBl 1984/448</td>
</tr>
<tr>
<td>VfGH</td>
<td>Verfassungsgerichtshof</td>
</tr>
<tr>
<td>VKrG</td>
<td>Verbraucherkreditgesetz BGBl I 2010/28</td>
</tr>
<tr>
<td>VwGH</td>
<td>Verwaltungsgerichtshof</td>
</tr>
<tr>
<td>WWW</td>
<td>World Wide Web</td>
</tr>
<tr>
<td>Z</td>
<td>Ziffer</td>
</tr>
<tr>
<td>zB</td>
<td>zum Beispiel</td>
</tr>
</tbody>
</table>
1 EINLEITUNG

Durch die fortwährende Aufzeichnung unserer Daten und Verhaltensweisen und die damit verbundene digitale Speicherung rückt das Thema Datenschutz immer mehr in den Vordergrund. Vor allem sind jene Daten, die im Internet für jedermann öffentlich zugänglich sind und womöglich sogar ohne eigene Zustimmung veröffentlicht wurden, aus datenschutzrechtlicher Sicht äußerst relevant. Sei es ein Zeitungsartikel mit namentlicher Erwähnung, die Firmenwebsite mit Abbildung der Mitarbeiter oder bloß der Facebook-Post eines Freundes mit entsprechender Verlinkung.


Das Internet Vergisst also nicht. Fraglich ist, inwieweit Menschen als Grundrechtsträger i.S.d. Grundrechts auf Privat- und Familienleben aber auch juristische Personen aus Sicht des UWG und UrhG ein Recht auf Vergessen haben.

Eine weitere Problematik kann sich bei der Verarbeitung der gespeicherten Daten von Suchmaschinen ergeben, die wiederum nicht den Inhalt selbst, sondern lediglich einen Verweis auf die Daten liefern. Der EuGH hat die Frage der Betreiberhaftung jüngst in einem umstrittenen Urteil richtungsweisend zugunsten des Betroffenen beantwortet. Inwieweit sich

---

1 Aus Gründen der besseren Lesbarkeit wird in dieser Diplomarbeit auf die gleichzeitige Verwendung der weiblichen und männlichen Sprachform verzichtet. Diese Formulierung bezeichnet jedoch stets Personen beider Geschlechter.
2 Vgl. Pkt. 5 Recht auf Löschung der Daten.
dies auch auf Unternehmen unter Berücksichtigung des unlauteren Wettbewerbs bzw der Verletzung von Urheberrechten anwenden lässt, soll Schwerpunkt dieser Diplomarbeit sein.

1.1 Begriffsbestimmungen
Um im Anschluss die Themen «Datenschutz im Internet» und «Recht auf Vergessen» umfassend erörtern zu können, bedarf es eingangs der Definition und Abgrenzung von in diesem Zusammenhang wichtigen Begriffen.

1.1.1 Personenbezogene Daten


Von diesen direkt personenbezogenen Daten gilt es, die indirekt personenbezogenen Daten zu unterscheiden. Diese können bei der Datenverwendung durch den Verarbeiter keiner bestimmten Person zugeordnet werden. Lediglich der Auftraggeber kann mit diesen indirekt personenbezogenen Daten eine Person bestimmen. Beispielsweise ist die Sozialversicherungsnummer ein solches indirekt personenbezogenes Datum. Der Sozialversicherungsträger kann anhand der Nummer die restlichen zur Person gehörenden Daten ermitteln, womit es sich letztendlich wieder um personenbezogene Daten handelt.
Einleitung

Die Unterscheidung zwischen direkt und indirekt bezogenen Daten ist vor allem für das Bestehen der Meldepflicht\(^7\) nach dem DSG wesentlich. Lediglich die Verarbeitung von indirekt personenbezogenen Daten ist nicht meldepflichtig iSd DSG.

1.1.2 Betroffener

Betroffener ist gem § 4 Z 3 DSG jede natürliche oder juristische Person bzw Personengemeinschaft, die nicht Auftraggeber ist und deren Daten verwendet werden. Unter Personengemeinschaften sind Gesellschaften iSd Unternehmensgesetzes wie zB OG, GmbH & Co KG etc, aber auch Gesellschaften nach bürgerlichem Recht, oder bloße Miteigentümerschaft nach ABGB zu verstehen. Nach hA können auch Bürgerinitiativen und Hausgemeinschaften Betroffene iSd DSG sein.\(^8\)

Betroffene haben nach dem DSG höchstpersönliche Rechte wie etwa das Recht auf Geheimhaltung, Recht auf Information und Auskunft (§ 26 DSG), Recht auf Richtigstellung und Löschung (§ 27 DSG) sowie das Widerspruchsrecht gem § 28 DSG. Vor allem das Recht auf Löschung nach § 27 DSG wird unten\(^9\) im Detail behandelt.

Im DSG 1978 wurde durch die Novelle 1986 der Begriff des Betroffenen insoweit eingeschränkt, als juristische Personen öffentlichen Rechts und deren Organe keine Betroffenen waren. Diese Einschränkung wurde im DSG 2000 idgF aber nicht übernommen, da nach dem neuen Datenschutzgesetz alle personenbezogenen Daten zu schützen sind.\(^10\)

1.1.3 Auftraggeber

Der Auftraggeber ist iSd § 4 Z 4 DSG eine natürliche oder juristische Person, ein Organ einer Gebietskörperschaft, ein Amt oder eine Gesellschaft, die personenbezogene Daten zu einem bestimmten Zweck verarbeitet. Er entscheidet, was mit den Daten passiert und trägt somit auch die Verantwortung für die Datenverarbeitung und dafür, dass entsprechende Bestimmungen, wie etwa die des DSG, eingehalten werden. Wenn auch für die tatsächliche Verarbeitung Dienstleister iSd DSG herangezogen werden, bleibt die Auftraggeber-Eigenschaft beim Besteller der Dienstleistung.\(^11\)

Er besitzt auch das Verfügungsrecht über die Daten, sodass jederzeit eine Löschung, Richtigstellung bzw Auskunft begehrt werden kann.

---

\(^7\) Vgl Pkt 2.2.2 DVR und Meldepflicht.

\(^8\) *Dohr/Pollirer/Weiss/Knyrim, DSG*\(^2\) § 4 (Stand: 2.7.2014, rdb.at).

\(^9\) Vgl Pkt 5 Recht auf Löschung der Daten.

\(^10\) *Dohr/Pollirer/Weiss/Knyrim, DSG*\(^2\) § 4 (Stand: 2.7.2014, rdb.at).

\(^11\) *Sonntag, Einführung in das Internetrecht*\(^2\) (2014), 224.
1.1.4 Dienstleister
Dienstleister sind hingegen nur Hilfsorgane, die den Auftraggeber bei der technischen Umsetzung unterstützen. Primär sind darunter natürliche und juristische Personen zu verstehen, die Dienstleistungen iSd § 153 GewO erbringen. Aber auch alle anderen Personen sowie Personengesellschaften und Gebietskörperschaften, die vom Auftraggeber überlassene Daten zur Herstellung eines Werkes verwenden – also verarbeiten bzw. übermitteln – sind Dienstleister iSd DSG.


Der Dienstleister verliert seine Eigenschaft als Dienstleister und wird selbst zum Auftraggeber, wenn er für die ihm überlassenen Daten ein Entgelt leistet, die Daten von verschiedenen Auftraggebern verknüpft oder wenn er die Daten entgegen der Anordnung des Auftraggebers verwendet oder über deren Verwendung selbst entscheidet.\(^\text{12}\)

1.1.5 Datenverarbeitung

Die Datenübermittlung ist iSd DSG die bloße Weitergabe der Daten an andere Empfänger als Auftraggeber und Betroffener. Das entscheidende Merkmal ist dabei die Änderung des Verwendungszweckes der Daten. So ist beispielsweise die Veröffentlichung von Daten eine Form der Übermittlung. Die Auskunft an den Betroffenen bzw die Weitergabe zur Verarbeitung stellt aber eben keine Übermittlung dar. Es ist davon die «Überlassung» der Daten an einen Dienstleister zu unterscheiden, die eine spezielle Art der Verarbeitung darstellt, und für die die strengeren Vorschriften gelten. Der Unterschied zur Übermittlung besteht darin, dass bei der

\(^{12}\) Dohr/Pollirer/Weiss/Knyrim, DSG\(^2\) § 4 (Stand: 2.7.2014, rdb.at).

Überlassung eine natürliche oder juristische Person beauftragt wird, die Daten vereinbarungsgemäß an Stelle des Auftraggebers zu verarbeiten.\textsuperscript{14}

Jede beliebige Verwendung von Daten, die eben keine Übermittlung ist, stellt eine Form der «Verarbeitung» dar. Dies kann beispielsweise die Ermittlung, Überlassung, Speicherung, Veränderung, Löschung, Vernichtung, etc sein. Da die Verarbeitung eher das Grundrecht auf Datenschutz verletzen kann, gelten hierfür besondere Vorschriften. Deshalb wurde die Übermittlung im DSG auch aus der Verarbeitung ausgeschieden.

1.2 Entwicklung des Datenschutzes in Österreich


Wegen der Zunahme der grenzüberschreitenden Übermittlungen von personenbezogenen Daten und dem vermehrten Austausch der Daten zwischen den in verschiedenen Mitgliedstaaten der EU niedergelassenen Unternehmen wurde 1995 die Datenschutz-Richtlinie 95/46/EG beschlossen. Da die unterschiedlichen Schutzniveaus der Rechte und Freiheiten von Personen hinsichtlich der Verarbeitung personenbezogener Daten eine Übermittlung in einen anderen Mitgliedstaat einschränken bzw verhindern konnten, dies wiederum den Wettbewerb verfälschte und dadurch Wirtschaftstätigkeiten auf Gemeinschaftsebene gehemmt werden konnten, war die Schaffung eines gleichwertigen Schutzniveaus hinsichtlich der Rechte und Freiheiten von Personen bei der Verarbeitung dieser Daten in allen Mitgliedstaaten unerlässlich. In diese EU-Richtlinie wurden die jeweils strengsten und umfassendsten Bestimmungen der einzelnen Mitgliedstaaten aufgenommen.\textsuperscript{15}

Nicht zu vergessen ist in diesem Zusammenhang auch die Datenschutzkonvention des Europarates, die am 30.6.1988 im BGBl Nr. 317/1988 kundgemacht wurde, die durch die EU-Richtlinie noch weiter konkretisiert und erweitert wurde.


\textsuperscript{14} Unger, Grundzüge des Datenschutzrechts\textsuperscript{2} (2015), 8.
\textsuperscript{15} Dohr/Pollirer/Weiss/Knyrim, DSG\textsuperscript{2} Erläuterungen zum „Datenschutzdreieck“ (Stand: 2.7.2014, rdb.at).

Letztendlich sind noch die E-Commerce-Richtlinie 2000/31/EG (im Folgenden ECRL genannt) vom 8.6.2000, die die Mitgliedstaaten dazu verpflichtet, den Abschluss von Verträgen auf elektronischem Weg gesetzlich zu ermöglichen, sowie das ECG, das eben diese Richtlinie in österreichisches Recht umsetzt, zu beachten.
2 RECHTSGRUNDLAGEN

2.1 EU-Datenschutz-Richtlinie 95/46/EG


Die Datenschutz-Richtlinie fordert also den Schutz personenbezogener Daten natürlicher Personen von privaten und öffentlichen Datenverarbeitern bzw. Dienstleistern bei der automatisierten Datenverarbeitung.\(^\text{16}\)

2.2 Datenschutzgesetz 2000 (DSG)


2.2.1 Grundrecht auf Datenschutz

Ein Grundrecht ist ein subjektives verfassungsgesetzlich gewährleistetes Recht, das mit einer gewissen Unverbrüchlichkeit ausgestattet und rechtlich durchsetzbar ist.\(^\text{17}\)

Neben Art 8 MRK, der bereits eine allgemeine Garantie und auch Vorkehrungen gegen bestimmte Informationseingriffe enthält, ist in § 1 DSG das jedermann gewährleistete

---

\(^\text{16}\) Genz, Datenschutz in Europa und den USA (2004), 19.
\(^\text{17}\) Hengstschläger/Leeb, Grundrechte\(^2\) (2013), Rz 1/1.
Verfassungsrecht auf Geheimhaltung und Schutz seiner personenbezogenen Daten verankert. Dieses höchsterleichtliche und somit nicht vererb- und übertragbare Recht gewährt den Anspruch auf Geheimhaltung personenbezogener Daten sowie die Nebenrechte auf Auskunft, Richtigstellung und Löschung und ein Widerspruchsfahigkeit vorgesehenen Datenverwendungen.  

Das Datenschutzrecht ist ein Menschenrecht. Es steht jedermann zu und ist nicht an das Bestehen einer bestimmten Staatsbürgerschaft oder der Unionsbürgerschaft (Art 20 AEUV und Art 9 EUV) geknüpft, wobei jedermann in dieser Hinsicht auch geschlechterneutral zu verstehen ist. Nachdem aber neben Daten der Privatsphäre natürlicher Personen auch Wirtschaftsdaten personenbezogene Daten iSD § 1 DSG sein können, werden auch juristische Personen zu den Grundrechtsträgern gezählt.


Ausgenommen davon ist das Recht auf Auskunft, da hierfür in jedem Fall die Datenschutzbehörde zuständig ist.

Das Grundrecht auf Datenschutz schützt lediglich personenbezogene Daten, sofern diese einer bestimmten Person zugeordnet werden können und auch nur dann, sofern ein subjektives Interesse an der Geheimhaltung nachgewiesen werden kann und dieses Interesse auch objektiv schutzwürdig ist. Ob ein Geheimhaltungsinteresse besteht, ist im Einzelfall durch eine Interessensabwägung zu beurteilen, wobei die allgemeine Zugänglichkeit der Daten im Zeitpunkt der beabsichtigten Verwendung eine zentrale Rolle spielt. Öffentliche Daten unterliegen demnach nicht dem Datenschutz, wenn sie im Zeitpunkt der Verarbeitung frei
zugänglich sind, da es am schutzwürdigen Geheimhaltungsinteresse mangelt. Somit sind beispielsweise Daten aus dem öffentlichen Telefonbuch nicht geschützt, Geheimnummern hingegen schon, soweit sie im Zeitpunkt vor der Veröffentlichung nicht allgemein verfügbar waren.

2.2.1.1 Beschränkungen des Grundrechts

Wie fast jedes Grundrecht kann auch das Grundrecht auf Datenschutz unter bestimmten Voraussetzungen durch Eingriffe beschränkt werden, auch dann, wenn nach Abwägung der Interessen und Berücksichtigung aller Umstände ein schutzwürdiges Geheimhaltungsinteresse besteht.\(^{25}\)

Beschränkungen des Geheimhaltungsanspruchs sind nur in den Fällen des § 1 Abs 2 DSG zulässig, wobei Eingriffe einer staatlichen Behörde überdies nur aufgrund von Gesetzen erfolgen dürfen, die aus den in Art 8 Abs 2 MRK genannten Gründen notwendig sind. Im Fall einer zulässigen Beschränkung darf der Eingriff dabei nur in der jeweils günstigsten Art vorgenommen werden.


Der Betroffene muss über den Zweck informiert sein, sodass er die Vor- und Nachteile abwägen und ggf die Zustimmung verweigern oder widerrufen kann. Es ist dabei anzugeben, welche Daten verwendet werden und für welche Verarbeitung die Daten genutzt werden.

Eine weitere Ausnahme besteht bei der privaten Verarbeitung durch eine natürliche Person ausschließlich für persönliche oder familiäre Zwecke, wie z.B. Führen eines persönlichen Adress- bzw Telefonverzeichnisses, wenn die Daten durch rechtmäßige Übermittlung erhalten wurden.

\(^{24}\) Vgl OGH 28.11.2013, 6 Ob 165/13b, DAKO 2015/16.
Da das Grundrecht unter materiellem Gesetzesvorbehalt steht, kann auch der einfache Gesetzgeber weitere Ausnahmen schaffen, die jedoch den Anforderungen des Art 8 Abs 2 MRK genügen müssen. Dies ist dann der Fall, wenn besondere Interessen des Betroffenen selbst oder Interessen Dritter dem schutzwürdigen Geheimhaltungsinteresse überwiegen. Weiters muss die Ausnahme durch Gesetz erfolgen und ist nur in den in Abs 2 genannten Gründen zulässig.

**Art 8 Abs 2 MRK** Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.

Letztendlich gibt es neben den **sonstigen Ausnahmen im Staatsinteresse** (zB Schutz der verfassungsmäßigen Einrichtungen, Sicherstellung der Einsatzbereitschaft des Bundesheeres, Vorbeugung, Verhinderung, oder Verfolgung von Straftaten, etc) auch noch die Ausnahme des Rechts auf Datenschutz wegen **wissenschaftlicher Forschung und Statistik**: Für konkrete statistische Untersuchungen und wissenschaftliche Forschungen dürfen öffentlich zugängliche Daten sowie Daten, die vom Auftraggeber für andere Zwecke zulässigerweise ermittelt wurden und Daten, die für den Auftraggeber bloß indirekt personenbezogen sind, verwendet werden, sofern keine personenbezogenen Ergebnisse erzielt und veröffentlicht werden.

### 2.2.2 DVR und Meldepflicht


---

27 Dadurch wird der Gesetzgeber nur insoweit zu Beschränkungen ermächtigt, als damit ein ausdrücklich angeführtes legitimes Ziel verfolgt wird.
28 [Dohr/Pollirer/Weißen/Knyrim, DSG](https://www.dsg.2.at) § 1 (Stand: 2.7.2014, rdb.at).
29 [Sonntag, Einführung in das Internetrecht](https://www.dsg.2.at) (2014), 240.
30 [Unger, Grundzüge des Datenschutzrechts](https://www.dsg.2.at) (2015), 50.
31 Vgl § 16 Abs 2 DSG.
Elektronische Datenverarbeitungen sind grundsätzlich vom Auftraggeber bei der DSB zu melden, sofern keine Ausnahme nach § 17 Abs 2 oder 3 DSG besteht. Diese Meldung hat entsprechend § 17 DSG vor der Aufnahme einer Datenverarbeitung zu erfolgen und ist aktuell zu halten. Spätere Änderungen oder Ergänzungen sind ebenso zu melden wie nicht mehr durchgeführte Datenverarbeitungen vom Auftraggeber streichen zu lassen (§ 22 Abs 3 DSG). Bei Nichtbeachtung drohen iSd § 52 Abs 2 Z 1 DSG Verwaltungsstrafen bis € 10.000.


Bei der erstmaligen Registrierung wird an den Auftraggeber eine siebenstellige DVR-Nummer vergeben, die für diesen immer gleich bleibt und auf den Geschäftspapieren anzuführen ist.

2.2.2.1 Ausnahmen von der Meldepflicht

In § 17 Abs 2 DSG werden bestimmte Ausnahmen für die Meldepflicht von automatisationsunterstützt verarbeiteten Daten definiert. Demnach sind Datenanwendungen, die ausschließlich veröffentlichte Daten enthalten (zB Telefonbuch) oder auch Register und Verzeichnisse, die von Gesetzeswegen einsehbar sind, zB Grundbuch, Firmenbuch, Vereinsregister, etc von der Meldepflicht ausgenommen. Ebenso sind Datenanwendungen, die nur indirekt personenbezogene Daten enthalten oder von natürlichen Personen ausschließlich für persönliche oder familiäre Zwecke durchgeführt werden, nicht meldepflichtig. Weiters sind jene Daten, die für publizistische Tätigkeiten verwendet werden, iSd § 48 DSG nach dem sog Medienprivileg meldungsfrei, sofern es sich um Daten handelt, die für die Ausübung des Grundrechts auf freie Meinungsäußerung gem Art 10 EMRK erforderlich sind.

Letztendlich gibt es noch eine Ausnahme von der Meldepflicht, wenn eine Standardanwendung vorliegt. Der Bundeskanzler kann per Verordnung für jene Fälle eine Standardanwendung definieren, in denen Datenanwendungen von vielen Auftraggebern in gleicher Weise mit

32 Unger, Grundzüge des Datenschutzrechts² (2015), 55.
34 Unger, Grundzüge des Datenschutzrechts² (2015), 58.
demselben Inhalt oder Übermittlungen routinemäßig durchgeführt werden und gleichzeitig die
schutzwürdigen Geheimhaltungsinteressen voraussichtlich nicht gefährdet werden.\textsuperscript{35}

\subsection{2.2.3 Rechtsschutz}
Werden die Bestimmungen des DSG nicht eingehalten, so sind neben den Verwaltungsstrafen
gem § 52 DSG die gerichtliche Geltendmachung, die Beschwerde und Anregung einer
Kontrolle an die DSB sowie die Geltendmachung allgemeiner Schadenersatzansprüche
möglich. Das Datenschutzrecht sieht somit grds ein zweigeteiltes Rechtsschutzsystem vor,
wonit die DSB (§§ 30 ff DSG) über Verletzungen im öffentlichen Bereich und die
Landesgerichte (§ 32 Abs 4 DSG) über Verletzungen des privaten Bereichs zu entscheiden
haben.

\subsubsection{2.2.3.1 Anregung einer Kontrolle an die DSB (§ 30 DSG)}
Mit der Umsetzung der Datenschutz-Richtlinie hat die Datenschutzbehörde als unabhängige
Kontrollstelle sowohl den privaten als auch den öffentlichen Bereich zu kontrollieren. Eine
Eingabe von Betroffenen an die DSB ist möglich, wenn sie durch einen Auftraggeber oder
Dienstleister in ihren subjektiven Rechten oder durch Nichteinhaltung der ihnen gegenüber
bestehenden Pflichten verletzt zu sein behaupten.\textsuperscript{36}

Im privaten Bereich ist zu berücksichtigen, dass Verletzungen des DSG nur bei den
Zivilgerichten durchgesetzt werden können. Die DSB ist in diesen Fällen lediglich
„Ombudsmann“ und kann Empfehlungen aussprechen, hat aber nicht die Befugnis, die Rechte
des Betroffenen durchzusetzen.

Eine Eingabe bei der DSB ist – im Gegensatz zur Klagseinbringung bei Gericht – ein von allen
Kosten befreites Verfahren. Eingaben sind binnen einem Jahr nach Kenntnis des Betroffenen
einzubringen (§ 34 Abs 1 DSG), wobei die absolute Verjährungsfrist drei Jahre beträgt (§ 1489
ABGB).

Die DSB ist bei begründetem Verdacht von Verletzungen des DSG gem Abs 2 auch von sich
aus berechtigt, die Datenanwendung zu prüfen. Der Auftraggeber kann einer solchen
Überprüfung weder ein Betretungsverbot noch Betriebs- und Geschäftsgeheimnisse
entgegenhalten. Die Einschau ist dabei nur unter möglichster Schonung der Rechte des
Auftraggebers bzw Dienstleisters möglich und bedeutet vor allem, dass dies nur innerhalb der
Betriebszeiten des Auftraggebers oder Dienstleisters vorgenommen werden darf.\textsuperscript{37}

\textsuperscript{35} Sonntag, Einführung in das Internetrecht\textsuperscript{2} (2014), 257.
\textsuperscript{36} Unger, Grundzüge des Datenschutzrechts\textsuperscript{2} (2015), 91.
\textsuperscript{37} Dohr/Pollirer/Weiss/Knyrim, DSG\textsuperscript{2} § 30 (Stand: 7.7.2015, rdb.at).
Das Ergebnis der Kontrolle ist die Aussprache von Empfehlungen zur Herstellung des rechtmäßigen Zustands, die mit einer Erledigungsfrist zu versehen sind. Wird die Empfehlung nicht fristgerecht umgesetzt, kann die DSB gem § 30 Abs 6 DSG

- Strafanzeige nach § 51 DSG oder § 52 DSG erheben
- Feststellungsklage beim zuständigen Zivilgericht erheben, wenn der begründete Verdacht einer schwerwiegenden Datenschutzverletzung durch einen privaten Auftraggeber besteht
- die Befassung der obersten Organe anordnen, wenn der Auftraggeber ein Organ einer Gebietskörperschaft ist.

2.2.3.2 Beschwerde an die DSB (§ 31 DSG)


Die Beschwerde ist gebührenfrei und hat schriftlich zu erfolgen. Sie ist wie bereits dargestellt binnen einem Jahr bei der DSB einzubringen, wobei die absolute Verjährungsfrist drei Jahre beträgt. Musterformulare für Auskunftsbeschwerden und allgemeine Beschwerden sind auf der Website der DSB zum Download bereitgestellt.


---

38 Bei Verletzungen der Gerichte ist Beschwerde innerhalb der Gerichtsbarkeit möglich, vgl OGH 28.11.2013, 6 Ob 165/13b, Dako 2015/16.

2.2.3.3 Anrufung der ordentlichen Gerichte (§ 32 DSG)


Die Datenschutzbehörde hat u.U auf Verlangen des Betroffenen als Nebenintervenient dem Verfahren beizutreten (§ 32 Abs 6 DSG).

2.2.3.4 Umweg über das UWG – strafrechtliche Verfolgung wegen Gewinn- oder Schädigungsabsicht durch die ordentlichen Gerichte (§ 51 DSG)

Sofern es sich um eine Verletzung der Datenschutzvorschriften im geschäftlichen Verkehr handelt, ein Konkurrenzverhältnis vorliegt und dadurch ein gewisser Einfluss auf die Marktposition der Mitbewerber ausgeübt wird, kann die Verletzung der Datenschutzvorschriften auch über Umwege des Wettbewerbsrechts sanktioniert werden. Eine weitere Voraussetzung dafür ist ein Verstoß gegen die guten Sitten iSd § 1 UWG oder eine unlautere Irreführung iSd § 2 UWG.

2.3 E-Commerce Gesetz (ECG)


---

41 Unger, Grundzüge des Datenschutzrechts² (2015), 94.
42 Sonntag, Einführung in das Internetrecht² (2014), 258.
43 Jahnel/Thiele, Datenschutz durch Wettbewerbsrecht, ÖJZ 2004/55.
jene Bestimmungen näher erläutert, die im Zusammenhang mit dem „Recht auf Vergessen werden bei Suchmaschinen“ relevant sind.

2.3.1 Ausschluss der Verantwortlichkeit bei Suchmaschinen (§ 14 ECG)

§ 14 ECG regelt dabei im Speziellen die Verantwortlichkeit bei Suchmaschinen, bzw den Ausschluss der Verantwortlichkeit, sofern nämlich der Diensteanbieter die Übermittlung der abgefragten Informationen nicht veranlasst, den Empfänger nicht auswählt und die abgefragten Informationen weder auswählt noch verändert.

2.3.2 Herkunftslandprinzip und seine Ausnahmen (§§ 20 ff ECG)


2.4 Künftiges EU-Datenschutzrecht (DSGVO)


Eine wesentliche Neuerung soll die Erhöhung der Strafen darstellen. Während derzeit das DSG Strafen iHv € 25.000,- als Maximalstrafe normiert, sieht der Entwurf der DSGVO Geldbußen bis zu € 1 Mio oder alternativ bis zu 2 % des weltweiten Jahresumsatzes eines Unternehmens vor – je nachdem, was höher ist. Das Europäische Parlament fordert aber einen noch höheren Strafrahmen von € 100 Mio bzw 5 % vom Konzernumsatz. Die Strafen sind von der

45 Knyrim, Datenschutzrecht (2015), 8.
Aufsichtsbehörde, in Österreich also von der Datenschutzbehörde und nicht mehr von den Bezirksverwaltungsbehörden bzw. Magistraten zu verhängen.\textsuperscript{48}

Das Reformpaket der EU, das die EU-Kommission schon im Jahr 2012 vorgeschlagen hat, besteht aus

1. einem Vorschlag für eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr\textsuperscript{49} und

2. einem Vorschlag für eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr\textsuperscript{50}.


Anders als das DSG schützt die DSGVO nur Daten von natürlichen Personen und erstreckt sich nicht auch auf juristische Personen.\textsuperscript{51}

Der örtliche Anwendungsbereich wurde heftig diskutiert und scheint noch nicht abschließend geklärt zu sein. Nach Art 3 der DSGVO soll die Verordnung nicht nur auf Auftraggeber oder Dienstleister anwendbar sein, die ihren Sitz innerhalb der EU haben oder ihre Aktivitäten innerhalb der EU durchführen, sondern auch auf alle Datenverarbeitungen, die von Auftraggebern außerhalb der EU an Betroffene innerhalb der EU erbracht werden. Dies, wenn die Ware oder Dienstleistung von einem Drittstaat angeboten wird oder das Verhalten des Betroffenen außerhalb der EU überwacht wird.\textsuperscript{52} Durch diese Erweiterung des Anwendungsbereichs sollen auch große US-Anbieter wie etwa Google dem europäischen Datenschutzrecht unterworfen werden. Für europäische Unternehmen und Bürger hätte dies den

\textsuperscript{48} Knyrim, Datenschutzrecht\textsuperscript{3} (2015), 24.
\textsuperscript{51} Skopik, Cyber Attack Information System (2015), 205.
\textsuperscript{52} Knyrim, Datenschutzrecht\textsuperscript{3} (2015), 12.

Die **Grundprinzipien der Datenverarbeitung** iSd Art 5 DSGVO sind bereits aus der Datenschutz-Richtlinie und § 6 DSG bekannt. Lediglich der Vorschlag des Rates der EU, das Prinzip der Datenminimierung zu streichen, würde einen bedeutenden Paradigmenwechsel bedeutet\(^{53}\), falls dieser Vorschlag umgesetzt wird, auf den hier aber nicht näher eingegangen wird.

Art 17 regelt künftig das geradezu überstrapazierte **Recht auf vergessen werden**\(^{54}\), das auf ein etwas erweitertes Löschungsrecht reduziert wird. Es soll also weiterhin ein Löschungsrecht geben, sofern dieses begründet ist, mit der Erweiterung, dass den Auftraggeber eine Informationspflicht trifft, wenn er Daten von Betroffenen an Dritte weitergibt und diese eine Lösung verlangen. Er muss den Dritten also darüber informieren, dass der Betroffene eine Lösung verlangt. Dies wurde im geleakten Entwurf des Rates in Art 17 Abs 2a aber wieder deutlich eingeschränkt hinsichtlich verfügbarer Technologien, vertretbarem Aufwand und Implementierungskosten. Wie diese Informationspflicht in der Praxis also umgesetzt wird, bleibt abzuwarten.\(^{55}\)

Am 15. Dezember 2015 erzielten Rat, Parlament und Kommission im Trilog eine Einigung, die der Ausschuss der Ständigen Vertreter (AStV) bestätigte. Die wichtigsten Eckpfeiler sind neben den gestärkten Bürgerrechten und dem verringerten Verwaltungsaufwand auch Vorschriften für die Anpassung der Unternehmen an das digitale Zeitalter. Unternehmen sollten sich schon deshalb früh genug mit der Umsetzung der Verordnung befassen und entsprechende Datenschutz-Maßnahmenpakete schnüren, um hohe Geldstrafen zu vermeiden.\(^{56}\)

Der ursprüngliche Entwurf sieht in Art 91 Z 2 vor, dass die europäische Datenschutzreform 20 Tage nach ihrer Publikation im Amtsblatt der EU in Kraft tritt. Um den Unternehmen und öffentlichen Einrichtungen aber eine entsprechende Frist zur Vorbereitung zu gewähren, soll die Anwendbarkeit erst zwei Jahre nach der Publikation gegeben sein.

Nach Überarbeitung durch die Rechts- und Sprachsachverständigen wird die DSGVO dem Rat und dem Parlament zur Annahme vorgelegt und voraussichtlich im Frühjahr 2018 in Kraft treten.

---

\(^{53}\) Vgl Art 5 Z 1 lit c des Ratsentwurfes vom 11.6.2015 „limited to the minimum necessary“ soll gestrichen und durch „not excessive“ ersetzt werden.

\(^{54}\) Vgl Pkt 4 EuGH-Urteil C-131/12.

\(^{55}\) Knyrim, Datenschutzrecht\(^{3}\) (2015), 22.

\(^{56}\) Knyrim, Datenschutzrecht\(^{3}\) (2015), 30.
3 Datenschutz im Internet

3.1 Datenschutzbehörde

Art 28 Abs 1 der Datenschutz-Richtlinie sieht vor, dass jeder Mitgliedstaat eine oder mehrere öffentliche Kontrollstellen einzurichten hat, die die Anwendung der einzelstaatlichen Vorschriften überwachen. In Österreich war dies bis 2014 die Datenschutzkommission.

Im Zuge der Verwaltungsgerichtsbarkeits-Novelle 2012\(^{57}\) wurde die Auflösung der unabhängigen Verwaltungsbehörden – darunter auch die Datenschutzkommission – beschlossen. Um den unionsrechtlichen Vorgaben zu entsprechen, wurde per 1. Jänner 2014 die neue Kontrollstelle iSd § 36 DSG, nämlich die Datenschutzbehörde, eingerichtet.\(^{58}\)

Die DSB ist anders als die Datenschutzkommission eine Behörde mit einem Leiter und kein Kollegialorgan mehr.\(^{59}\) Dr. Andrea Jelinek wurde auf Vorschlag der Bundesregierung vom Bundespräsidenten für fünf Jahre zur Leiterin der DSB bestellt.\(^{60}\) Die DSB ist zur Wahrung des Datenschutzes sowohl im öffentlichen als auch im privaten Bereich berufen und hat vorwiegend Kontroll- und Entscheidungsbefugnisse. Die Mitglieder der DSB sind gem § 37 Abs 2 DSG weisungsfrei und auch zur Kontrolle der obersten Vollzugsorgane ermächtigt. Sowohl Bundespräsident, Bundesregierung, einzelne Bundesminister als auch die Mitglieder der Landesregierungen unterliegen ihrer Kontrolle, so dass man in gewisser Weise von einem Höchstgericht sprechen kann.\(^{61}\)

Zu den Aufgaben\(^{62}\) der DSB zählen neben der Führung des Datenverarbeitungs- und des Stammzahlenregisters hauptsächlich die Behandlung von Eingaben von Personen, die sich in ihren Rechten auf Datenschutz verletzt erachten iSd § 31 DSG und das Kontroll- und Ombudsmannverfahren nach § 30 DSG.

Die DSB kann eine Kontrolle der Datenverwendung vornehmen, wenn entweder eine Person behauptet, in ihren Rechten verletzt worden zu sein oder begründeter Verdacht einer solchen


\(^{58}\) Skopik, Cyber Attack Information System (2015), 203.


\(^{60}\) Wähltbar sind alle Frauen und Männer, die am Stichtag das passive Wahlrecht iSd § 41 Abs 1 1. Satz NRWO besitzen. Auch eine mehrmalige Wiederbestellung ist möglich.


Verletzung besteht, sowie in bestimmten Konstellationen auch ohne Verdacht. Letzteres ist bei Anwendungen, die der Vorabkontrolle nach § 18 Abs 2 DSG unterliegen, der Fall, wenn es sich um keine Musteranwendung handelt und strafrechtliche oder sensible Daten verarbeitet werden oder diese Daten die Kreditwürdigkeit betreffen.\(^{63}\)

Im Falle des begründeten Verdachts muss die DSB die Datenanwendung prüfen. Dies hat unter größtmöglicher Schonung der Rechte des Auftraggebers und somit nur innerhalb der Betriebszeiten zu erfolgen, wobei der Auftraggeber die notwendige Unterstützung\(^{64}\) zu leisten hat. Es können auch keine Einwände aufgrund Geschäfts- oder Betriebsgeheimnisse geltend gemacht werden.

Im Rahmen des Beschwerdeverfahrens auf Antrag nach § 31 DSG hat die DSB ggf eine Rechtsverletzung mit Bescheid festzustellen. Rechtsmittelinstanz ist das BVwG, das die Bescheide der DSB gem § 39 DSG iVm Art 135 Abs 1 B-VG und § 6 BVwGG prüft. Betroffene, die nach § 31 DSG die Datenschutzbehörde wegen Verletzung ihrer Rechte anrufen, können nunmehr die Entscheidung der DSB mittels Beschwerde beim BVwG bekämpfen. Gegen Erkenntnisse des BVwG ist letztendlich Revision beim VwGH zulässig. Hingegen kann die DSB beim Kontroll- und Ombudsmannverfahren nach § 30 DSG lediglich Empfehlungen aussprechen und keine Bescheide erlassen.


Auf der Internetseite\(^{65}\) der DSB werden allgemeine Informationen zu Verfahren vor der DSB sowie Musterformulare zur Verfügung gestellt.

### 3.2 Datenschutzbeauftragter

Sowohl in der DSG-Novelle 2008\(^{66}\), als auch in der DSG-Novelle 2012\(^{67}\) war bereits die gesetzliche Einführung eines bDSB geplant. Dies ist aber beide Male am Widerstand der Wirtschaftskammer Österreich gescheitert.\(^{68}\)

\(^{63}\) *Sonntag*, Einführung in das Internetrecht\(^{2}\) (2014), 265.

\(^{64}\) Dies betrifft va Erklärungen zum Ablauf der Datenanwendung, Bekanntgabe von Passwörtern, etc.


\(^{66}\) 182/ME XXIII.GP.

\(^{67}\) 397/ME XXIV.GP.

Im Entwurf der EU-Kommission für die DSGVO ist die Einführung eines verpflichteten bDSB ab einer Unternehmensgröße von mehr als 250 Mitarbeitern wieder vorgesehen. Das Europäische Parlament hingegen fordert schon einen bDSB, sofern der Auftraggeber die Daten von mehr als 5.000 betroffene Personen speichert,\(^\text{69}\) wohingegen der Rat der EU es jedem Mitgliedstaat frei stellen will, ob er die Einrichtung eines verpflichteten bDSB vorsieht. Welche Regelung die neue DSGVO enthalten wird, hängt also weiterhin von den politischen Diskussionen ab und bleibt gespannt abzuwarten.\(^\text{70}\)

Jedoch erscheint es auch ohne gesetzliche Verpflichtung sinnvoll, einen bDSB zu bestellen, da dieser dabei helfen soll, jene Risiken, die durch Datenschutzverletzungen entstehen können, für das Unternehmen zu minimieren. Er sollte längerfristig bestellt werden, um eine planvolle Ausübung seiner Tätigkeiten zu ermöglichen.

Sofern es sich um einen internen Mitarbeiter handelt, soll er in der Funktion als bDSB jedenfalls weisungsfrei und eigenständig handeln können.\(^\text{71}\) Empfehlenswert ist die schriftliche Bestellung zum Datenschutzbeauftragten, die wohl nur mit freiwilliger Zustimmung des Arbeitnehmers möglich ist.

### 3.2.1 Kompetenzen und Fähigkeiten des bDSB

Die Position bzw Funktion ist eine anspruchsvolle und erfordert neben Fachkenntnissen in Recht, IT und Betriebswirtschaft auch persönliche Fähigkeiten wie Lösungskompetenz, Unbescholtenheit, Zuverlässigkeit und Lernbereitschaft.\(^\text{72}\) Der bDSB ist mit entsprechenden Kompetenzen auszustatten und, wenn möglich, als Stabstelle einzurichten und direkt der Geschäftsleitung zu unterstellen. Um seine Aufgaben im Interesse des Unternehmens ausüben zu können, ist ein Einsichtsrecht in sämtliche relevante Unterlagen zu gewähren und die Zurverfügungstellung entsprechender Mittel, Geräte und Einrichtungen erforderlich.

### 3.2.2 Aufgabengebiete des bDSB

Der tatsächliche Aufwand reicht bei datenverarbeitungsintensiven Unternehmen von 20 % der Arbeitszeit bis zur Vollzeitbeschäftigung.\(^\text{73}\) Die Hauptaufgabe besteht in der Überwachung der

---

\(^{69}\) Diese Ansicht wird heftig kritisiert, da mit dieser Regelung alle Unternehmer einen bDSB bestellen müssen, die mehr als 5.000 Kundendatensätze speichern. Dazu zählt beispielsweise schon der Pizza-Lieferant, der einen Newsletter an 5.000 Empfänger schickt.

\(^{70}\) Vgl Pollirer, Die Datenschutz-Grundverordnung: Der Datenschutzbeauftragte, Dako 2015,65.

\(^{71}\) Knyrim, Datenschutzrecht\(^2\) (2015), 355.

\(^{72}\) Vgl „Das berufliche Leitbild des Datenschutzbeauftragten“, Stand Juni 2011, Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. Siehe weiters Pollirer, Der betriebliche Datenschutzbeauftragte in Österreich – Anforderungsprofil, Fähigkeiten und Kenntnisse, Dako 2014,10.

\(^{73}\) Für das Beispiel des bDSB der Erste Group Bank AG siehe das Interview von Schmidt/Knyrim, mit König, Der Mensch ist die größte Schwachstelle, Dako 2015,26.
Einhaltung aller datenschutzrechtlichen Vorschriften. Verletzungen des Datenschutzrechts können für das Unternehmen schwerwiegende Folgen haben, nämlich Verwaltungsstrafen bis zu € 25.000 gem § 52 Abs 1 DSG, immateriellen Schadenersatz nach § 33 DSG bis zu € 20.000, materiellen Schadenersatz in unbestimmter Höhe und nicht zuletzt schwerwiegende Imageschäden, die im schlimmsten Fall zum Untergang des Unternehmens führen können. Auch auf die kommenden hohen Strafen nach der DSGVO sei nochmals verwiesen.\textsuperscript{74}

### 3.3 Vorratsdatenspeicherung

Unter Vorratsdatenspeicherung ist die Speicherung von personenbezogenen Daten zu verstehen, die bei der Telekommunikation anfallen und für die Strafverfolgung verwendet werden sollen. Sie dient grds zur Aufklärung von schweren Straftaten. Die Daten werden ohne konkreten Verdacht auf Vorrat gespeichert, um sie später für Ermittlungen verwenden zu können. Ziel ist die Speicherung von Verbindungs- und Ortungsdaten und nicht die Speicherung von Gesprächsinhalten.\textsuperscript{75}


Durch den NSA-Skandal\textsuperscript{77} im Jahr 2013 ist erneut die Diskussion um das richtige Verhältnis von Freiheit und Sicherheit im Internet entfacht. Befürworter sehen die Vorratsdatenspeicherung als entscheidendes Instrument zur Wahrung der Sicherheit im digitalen Zeitalter. Gegner betrachten sie hingegen als entscheidenden Schritt zum Überwachungsstaat. Das Thema ist sehr brisant und eine sachliche Diskussion scheint nahezu unmöglich.\textsuperscript{78}

\textsuperscript{74} Vgl Pkt 2.4 Künftiges EU-Datenschutzrecht (DSGVO).
\textsuperscript{75} https://www.dsb.gv.at/site/7713/default.aspx (Abfrage: 21.11.2015).
\textsuperscript{76} Richtlinie des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG.
\textsuperscript{77} Medien haben aufgrund der Informationen von Edward Snowden enthüllt, wie allumfassend die NSA und andere westliche Geheimdienste die weltweite Kommunikation überwachen.
\textsuperscript{78} Moser-Knierim, Vorratsdatenspeicherung Zwischen Überwachungsstaat und Terrorabwehr (2013), 180.
Am 27. Juni 2014 hat der VfGH die Bestimmungen über die Vorratsdatenspeicherung wegen unverhältnismäßigem Eingriff in das Grundrecht auf Datenschutz für verfassungswidrig erklärt und zur Aufhebung der Gesetze verpflichtet.\textsuperscript{79}

### 3.4 Systemanbieterhaftung

Eine wesentliche Frage bei dem riesigen Angebot an Informationen im Internet ist die Haftung dafür. Wer haftet für die Inhalte auf einer Website, für die Ergebnisse der Suchmaschine, für fremde Links, etc?

Eine konkrete Bestimmung über die Haftung ist weder dem DSG noch dem ECG als lex specialis zu entnehmen. In den §§ 13 ff ECG sind lediglich Bestimmungen über die Haftungsbeschränkungen bzw Haftungsausschlüsse geregelt. Liegen die Voraussetzungen des jeweiligen Tatbestands vor, so ist die Verantwortlichkeit sowohl in zivil- als auch in strafrechtlicher Hinsicht ausgeschlossen.\textsuperscript{80} Zankl sieht darin eine „horizontale Haftungsbeschränkung“\textsuperscript{81}. Gelangt man bei der Subsumtion zu keiner Haftungsbefreiung iSd §§ 13 ff ECG, so haftet also grds der Systemanbieter. Zu unterscheiden sind hierbei die **Access-Provider**, die dem User den Zugang zu einem Kommunikationsnetz ermöglichen und ausschließlich Transportleistungen anbieten, wie beispielsweise Mobiltelefonunternehmen oder ISP, und die **Hosting-Provider**, die es dem Kunden ermöglichen, Daten auf ihren Servern zu speichern. Typische Beispiele dafür sind Betreiber von E-Mail- und Webservern.\textsuperscript{82}

Vorab ist hervorzuheben, dass gem § 18 Abs 1 ECG keine generelle Überwachungs- und Nachforschungspflicht für Provider besteht. Anders ist dies in der Zwischenzeit aber, wenn bereits eine Rechtsverletzung vorgekommen ist (zB beleidigende Postings, illegal upgeladete urheberrechtlich geschützte Dateien, etc). Demnach liegt eine allgemeine, dh proaktive Überwachungspflicht sehr wohl vor, sobald Kenntnis einer besonderen und bereits realisierten Gefahr erlangt worden ist, die sich aber auf die konkreten Umstände (Personen, Themen, Musiktitel, etc) beschränkt.

### 3.4.1 Access-Provider

Access-Provider haften grds nicht, sofern sie die Übertragung nicht veranlasst haben. Eine Veranlassung ist dann gegeben, wenn eine explizite Zuleitung von nicht angeforderten Daten an bestimmte, vom ISP ausgewählte Personen erfolgt, wie beispielsweise die gezielte Anzeige

\textsuperscript{81} Zankl, E-Commerce-Gesetz in Sicht, AnwBl 2001, 459 (460).
\textsuperscript{82} Sonntag, Einführung in das Internetrecht\textsuperscript{2} (2014), 137.

3.4.2 Hosting-Provider

Bei Hosting-Provider ist die Haftungssituation gerade umgekehrt, da standardmäßig eine Haftung besteht und nur in besonderen Einzelfällen entfällt. Werden fremde Inhalte gespeichert, so ist er neben dem eigentlichen Urheber ebenso verantwortlich, wenn nicht ein besonderer Haftungsausschluss greift. Keine Haftung besteht ausnahmsweise, wenn der Hosting-Provider keine tatsächliche Kenntnis von rechtswidrigen Tätigkeiten oder Informationen hat, wobei er nicht verpflichtet ist, Auskünfte oder Rechtsgutachten über die Zulässigkeit einzuholen. Die Rechtswidrigkeit muss aber selbst für Laien offensichtlich sein.

Ein weiterer Haftungsausschluss besteht, wenn der Hosting-Provider zwar Kenntnis über die offensichtlich rechtswidrige Information besitzt, er aber unverzüglich zur Beseitigung des Zustands tätig wird. Es ist dabei entweder die Information zu entfernen (= Löschung) oder der Zugang zur Information zu sperren. Die Sperre ist in diesem Zusammenhang mit erheblichem Aufwand verbunden, da nach Ansicht des LG Hamburg im Falle von „Virtual Hosting“ eine Firewall oder Proxy zwischenzuschalten wäre, um eine bestimmte URL zu blockieren.

---

83 Analog dazu haftet auch der Buchhändler nicht als Störer von Urheberrechtsverletzungen. Es wäre ihm nicht zuzumuten, alle Bücher zu lesen. Auch eine Prüfpflicht ist ihm nicht zuzumuten, was auch wohl analog für Access-Provider gilt.
85 Sonntag, Einführung in das Internetrecht² (2014), 139.
86 Vgl OGH 6.7.2004, 4Ob 66/04s, Megasex.at: Nicht offensichtlich für juristische Laien sind: Keine oder ungültige AGBs, Mehrwertnummern ohne Preisangabe, fehlendes Impressum, arg „gratis“ als Beschreibung zu Mehrwertnummern.
87 Ist sehr streng auszulegen und beträgt bei Unternehmen ein bis zwei Stunden nach (Wieder-)Beginn der Geschäftszeiten.
88 Vgl LG Hamburg 31.7.2009, 325 O 85/09, MMR 2010, 60 (Ls.).
89 Sonntag, Einführung in das Internetrecht² (2014), 143.
3.5 Haftung für Links auf fremde Websites

Durch das bloße Verfolgen eines Hyperlinks begeht der User meist keine Urheberrechtsverletzungen. Deswegen kann in diesen Fällen auch das Setzen von derartigen Links keine Beihilfe zur Urheberrechtsverletzung darstellen.\textsuperscript{90} Anders ist dies, wenn man im Hyperlink die „Zurverfügungstellung“ nach § 18a UrhG sieht. Dies scheitert aber schon daran, dass der Linksetzer keinen Inhalt zur Verfügung stellt, denn wenn das Ziel verändert oder gelöscht wird, geht der Link ins Leere und der Inhalt ist nicht mehr erreichbar.\textsuperscript{91} Nach Handig setzt die Zurverfügungstellung die Speicherung auf einem Webserver voraus.\textsuperscript{92}

Meist erfolgt die Linksetzung auch, ohne den Rechtseinhaber um Erlaubnis zu fragen, was zur Folge hätte, dass nahezu das ganze WWW rechtswidrig wäre. Es wird dahingehend argumentiert, dass eine konkludente Zustimmung derer vorliegt, die Inhalte, auf die verlinkt werden kann, im Internet anbieten.\textsuperscript{93}

Eine Haftung des Linksetzers kann für die per Link erreichbare Inhalte dennoch in besonderen Fällen eintreten:\textsuperscript{94}

1. **Setzen eines verbotenen Links**: Sofern etwas verboten ist, stellt schon die bloße Werbung dafür eine Rechtswidrigkeit dar. Ein Link ist in diesem Fall als Werbung für die Sache zu qualifizieren.\textsuperscript{95}

2. **Bewusste Förderung von strafbaren Handlungen**: Links zu illegalen Seiten sind unzulässig, um dieser neue Besucher zuzuführen. Der Linksetzer haftet als Beitragstäter.

3. **„Zu-Eigen-Machen“ fremder Inhalte**: Wird der Inhalt der Zielseite als eigener bezeichnet oder in die eigene Webseite integriert, so haftet der Linksetzer wie für seine eigenen Inhalte.

Die Bestimmung des § 17 ECG normiert die Haftung für Links auf fremde Inhalte, wenn keine tatsächliche Kenntnis von der Rechtswidrigkeit der Information auf der Zielseite vorliegt, die erkennbar den Bestimmungen über den Haftungsausschluss von Host Providern nachgebildet worden ist. Ganz im Gegenteil zum Betreiber einer Suchmaschine sucht der Linksetzer bewusst den Inhalt der fremden Webseite und setzt manuell einen Link zu dieser Information. Ähnlich

\textsuperscript{90} Vgl LG München I 14.11.2002, 7 O 4002/02, MMR 2003, 197.
\textsuperscript{91} Gaderer in Kuczko, urheber.recht § 18a UrhG (Stand 1.12.2007, rdb.at).
\textsuperscript{92} Handig, Das Zurverfügungsstellungsrecht und die Hyperlinks ecolex 2004, 38.
\textsuperscript{93} Stomper, ÖBI 2002, 44; Stomper, MR 2003, 33.
\textsuperscript{94} Sonntag, Einführung in das Internetrecht\textsuperscript{2} (2015), 154.
\textsuperscript{95} Vgl LG München I 11.10.2006, 21 O 2004/06, MMR 2007, 128.


Der Haftungsausschluss iSd § 17 ECG soll nur dann greifen, wenn der Linksetzer die fremden Informationen nicht als seine eigenen darstellt. Es ist daher ratsam, den Nutzer deutlich darauf aufmerksam zu machen, dass der Link zu fremden Inhalten führt (=Disclaimer). Denn nur dann kann er sich auf § 17 ECG berufen und ist von der Haftung befreit.

### 3.6 Haftungsausschluss für Suchmaschinen


§ 14 ECG regelt den Ausschluss der Verantwortlichkeit für Suchmaschinen. Unter Suchmaschinen versteht der Gesetzgeber dabei jene Diensteanbieter, die eine elektronische
Suche nach Informationen durchführen. Voraussetzung für eine Haftungsbefreiung ist gem § 14 Abs 1 Z 3 ECG, dass der Betreiber der Suchmaschine die Inhalte weder auswählt noch verändert. Demnach sind nur automatisierte Suchen zu verstehen. Der Haftungsausschluss ist dabei durch die mangelnde Einflussmöglichkeit auf die Informationen in den Zielseiten durch den Betreiber der Suchmaschine begründet.

4 EuGH-Urteil C-131/12

In diesem richtungsweisenden Urteil vom 13.5.2014 wird das Löschungsrecht bei Suchmaschinen in bestimmten Situationen und unter bestimmten Voraussetzungen zugunsten des Betroffenen bejaht und verpflichtet den Suchmaschinenbetreiber zur Löschung aus dem Suchindex.

4.1 Sachverhalt

Im Jahr 1988 veröffentlichte die spanische Tageszeitung La Vanguardia zwei Bekanntmachungen zur Immobilienversteigerung wegen einer Pfändung infolge der Betreibung von Sozialversicherungsschulden des spanischen Rechtsanwalts Mario Costje González. In weiterer Folge wurde auch eine elektronische Ausgabe der Zeitung online gestellt.

Mehr als zehn Jahre später beanstandete der Betroffene beim Verleger der Zeitung, dass bei Eingabe seines Namens in der Google-Suchmaschine eine Verknüpfung zur genannten Bekanntmachung erscheine, das Pfändungsverfahren aber seit Jahren erledigt und nicht mehr von Relevanz sei. Der Verleger verweigerte allerdings die Löschung und berief sich auf das spanische Arbeits- und Sozialministerium, das derartige Veröffentlichungen anordnet.

Im Februar 2010 verlangte González bei Google Spain die Löschung der Verknüpfung zu der Zeitung bei Eingabe seines Namens in die Suchmaschine, die das Ersuchen an Google Inc. weiterleitete, da dieses Unternehmen die Internet-Suchdienste erbringe.


Hingegen wurde die Beschwerde gegen den Verleger mit der Begründung zurückgewiesen, dass die Veröffentlichung der Daten auf einer rechtlichen Grundlage erfolgt sei.

Google Inc. und Google Spain beantragten beim nationalen Obergericht in Spanien104 die Aufhebung der Entscheidung der AEPD. Im Zuge eines Vorabentscheidungsverfahrens wurde dem Europäischen Gerichtshof in diesem Zusammenhang eine Reihe von Fragen vorgelegt.

---

104 Audiencia Nacional de España ist der nationale Staatsgerichtshof in Spanien.
4.2 Schlussanträge des Generalanwalts

Niilo Jääskinen hielt als Generalanwalt fest, dass das Verarbeiten von personenbezogenen Daten im Rahmen der Tätigkeiten einer Niederlassung Hauptanknüpfungskriterium für den räumlichen Anwendungsbereich von nationalen Datenschutzvorschriften ist.

Die eigentliche Verarbeitung von personenbezogenen Daten erfolgt durch Google Inc., die auch die Suchmaschinendienste anbietet. Google Spain handelt lediglich als Vertreterin hinsichtlich Werbefunktionen, für die sie die Verarbeitung personenbezogener Daten ihrer spanischen Kunden übernimmt.

Das Geschäftsmodell von Suchmaschinenbetreibern beruht idR auf Schlüsselwörterwerbung, wodurch die kostenlose Bereitstellung der Suchmaschinendienste ermöglicht wird. Die meist für jedes Land gegründete Tochtergesellschaft ist daher jedenfalls mit der Internetsuchmaschine verbunden und stellt eine Präsenz am nationalen Werbemarkt dar.

Der Generalanwalt ist der Ansicht, dass dadurch jede Niederlassung jedenfalls personenbezogene Daten verarbeitet, sofern sie in Verbindung mit dem Dienst steht, der auf die zielgruppenspezifische Werbeeinschaltungen an die Bewohner des Mitgliedstaats ausgerichtet ist. Die nationalen Datenschutzbestimmungen sind demnach auf einen Suchmaschinenbetreiber anwendbar, wenn dieser im Mitgliedstaat eine Niederlassung zur Vermarktung und Verkauf von Werbeflächen einrichtet, die sich an die Bewohner des Mitgliedstaats richtet.


106 Der Urheber einer Webseite kann mit sog. ‚exclusion codes‘ der Suchmaschine den Befehl erteilen eine bestimmte Webseite nicht zu indexieren, zu speichern und bei den Suchergebnissen nicht anzuzeigen.

4.3 Kritische Betrachtung des Urteils

Die Tätigkeit von Suchmaschinen besteht darin, dass Daten, die von Dritten im Internet veröffentlicht wurden, gefunden, automatisch indexiert, vorübergehend gespeichert und letztendlich den Internetnutzern in einer bestimmten Reihenfolge ausgegeben werden.

Nach Art 2 lit b der Richtlinie 95/46/EG ist die automatische, kontinuierliche und systematische Durchforstung von Informationen im Internet eine Verarbeitung mithin von personenbezogenen Daten, da diese mit dem Indexprogramm ausgelesen, gespeichert, organisiert und dem Benutzer bereitgestellt werden. Dass die personenbezogenen Daten bereits zuvor im Internet veröffentlicht wurden und von der Suchmaschine nicht verändert werden, ändert nichts daran. Es ist auch dann von einer Verarbeitung auszugehen, wenn die Informationen genau so bereits in den Medien veröffentlicht worden sind.\textsuperscript{107}

Der Suchmaschinen-Dienstanbieter ist iSd Art 2 lit b der Richtlinie 95/46/EG Verantwortlicher, da er über die Verarbeitung selbst entscheidet. Außerdem ist unstreitig, dass er durch seine Tätigkeit einen maßgeblichen Anteil an der Verbreitung personenbezogener Daten hat, nämlich dadurch, dass er diese auch jenen Internetnutzern zugänglich macht, die diese Daten sonst nicht gefunden hätten.

Google Inc. betreibt die weltweite Google Search mit Sitz in den Vereinigten Staaten und hat für viele Länder eine lokale Version, die an die jeweilige Landessprache angepasst ist. Auf welchen Servern die Daten vorübergehend gespeichert werden, wird aus Wettbewerbsgründen geheim gehalten. Google Search zieht Gewinn aus dieser Tätigkeit, indem sie gegen Entgelt Werbeanzeigen einbettet. Damit eine Niederlassung iSd Art 4 Abs 1 lit a der Richtlinie 95/46/EG vorliegt, muss zumindest eine der vorliegenden Voraussetzungen erfüllt sein:

1. Der Suchmaschinenbetreiber gründet eine Zweigniederlassung oder Tochtergesellschaft, deren Tätigkeit auf die Bewohner des Mitgliedstaates gerichtet ist,
2. Google Inc. ernennt eine Tochtergesellschaft als Vertreterin im Mitgliedstaat und somit als Verantwortliche für die Datenverarbeitung, oder
3. Die jeweilige Zweigniederlassung bzw. Tochtergesellschaft leitet die Beschwerden und Anordnungen der nationalen Behörden und betroffenen Personen hinsichtlich

\textsuperscript{107} Vgl Satakunnan Markkinapörssi und Satamedia, C-73/07, EU:C:2008:727, Rn. 48 und 49.
Einhaltung des Rechts auf Schutz personenbezogener Daten an die außerhalb der Union ansässige Muttergesellschaft weiter, auch wenn dies freiwillig erfolgt.


4.4 Auswirkungen für den Suchmaschinenbetreiber

Art 12 lit b und Art 14 Abs 1 lit a der Richtlinie sind dahingehend auszulegen, dass der Suchmaschinenbetreiber zur Wahrung der Rechte iSd Datenschutz verpflichtet ist, sofern die Voraussetzungen erfüllt sind. Insofern ist er verpflichtet, Links aus der Ergebnisliste zu von Dritten veröffentlichten Daten zu entfernen, die nach Eingabe des Namens einer Person aufgelistet werden. Dies auch dann, wenn die Daten nicht gleichzeitig oder vorher auf der Quellseite gelöscht werden und ggf auch dann, wenn die Veröffentlichung auf der Webseite als solche rechtmäßig ist.\textsuperscript{108}

Es ist zu prüfen, ob der Betroffene ein Recht darauf hat, dass bestimmte Einträge im Index der Suchmaschine gelöscht werden. Es ist dabei nicht erforderlich, dass die betroffene Person durch die Einbeziehung des betreffenden Links in die Ergebnisliste dadurch einen Schaden erleiden könnte.

Die betroffene Person kann in Anbetracht ihrer Grundrechte iSd Art 7 und 8 der GRC verlangen, dass die betreffenden Daten der breiten Öffentlichkeit nicht mehr durch Einbeziehung in die Ergebnisliste einer Suchmaschine zugänglich gemacht werden. Dies ist immer dann der Fall, wenn das Interesse des Einzelnen jedenfalls das wirtschaftliche Interesse des Suchmaschinenbetreibers überwiegt und auch dann, wenn es das Interesse der breiten Öffentlichkeit am Zugang zu diesen Informationen überwiegt.

Bei Personen des öffentlichen Lebens kann das Interesse der breiten Öffentlichkeit aber überwiegen und eine Auflistung in den Suchergebnissen rechtfertigen.

\textsuperscript{108} EuGH, Urteil vom 13.5.2014, Rs. C-131/12, Rn 88.
5 RECHT AUF LÖSCHUNG DER DATEN

Gem § 27 DSG ist der Auftraggeber verpflichtet, unrichtige oder entgegen den Bestimmungen des DSG verarbeitete Daten richtigzustellen bzw zu löschen. Das nationale Datenschutzgesetz enthält somit schon Anknüpfungspunkte zur Datenlöschung.\textsuperscript{109} Unter Löschung versteht der OGH die physische Lösung, also die vollständige Vernichtung durch Zerstören oder Überschreiben. Bloßes logisches Löschen durch Auflösung einer Verknüpfung zu einem Datensatz reicht dazu nicht aus.\textsuperscript{110}

Der Richtigstellung bzw Löschung unterliegen Daten, deren Verarbeitung rechtlich unzulässig ist oder die unrichtig und somit falsch sind.\textsuperscript{111}

Die Frist für die Löschung bzw Richtigstellung beträgt wie die Frist für Auskunft gem § 26 DSG acht Wochen nach Einlangen des Antrags. Wird dem Antrag entsprochen, so ist der Betroffene darüber zu informieren. Wird dem Antrag hingegen nicht entsprochen, ist dies schriftlich zu begründen.\textsuperscript{112}

5.1 Löschung aus den Google-Suchergebnissen

Google hat nach dem EuGH-Urteil C-131/12 somit die Daten aus seinem Index zu löschen, sofern ein berechtigtes Interesse der betroffenen Person besteht. Durch dieses Urteil ist es möglich, die Löschung von Suchergebnissen zu verlangen, ohne sich an meist unbekannte Webseitenbetreiber in Drittstaaten wenden zu müssen.\textsuperscript{113}

Nachdem Google auch in Österreich eine Niederlassung unterhält, kann diese verpflichtet werden, einen Treffer aus dem Index zu löschen, auch wenn die Daten an der Quelle verfügbar bleiben.

5.1.1 Voraussetzungen und Löschungsantrag

Damit ein Link zu einer Seite mit personenbezogenen Daten gelöscht werden kann, bedarf es immer eines überwiegenden Interesses des Betroffenen. Es ist somit im Einzelfall eine Interessensabwägung zwischen Antragsteller und Suchmaschinenbetreiber durchzuführen und zu prüfen, ob die Daten der Suchergebnisse vom Informationsinteresse der Allgemeinheit gedeckt sind. Einem Löschungsantrag kann gerade bei Personen des öffentlichen Lebens das

\textsuperscript{109} Knyrim, Datenschutzrecht\textsuperscript{3} (2015), 326.
\textsuperscript{110} Vgl OGH 15.4.2010, 60641/10p.
\textsuperscript{111} Dohr/Pollirer/Weiss/Knyrim, DSG\textsuperscript{2} § 27 (Stand 2.7.2014, rdb.at).
\textsuperscript{112} Knyrim, Datenschutzrecht\textsuperscript{3}, 327.
\textsuperscript{113} Vgl Knyrim, Löschungsrecht bei Suchmaschinen, Dako 2014,11.

Voraussetzung für eine Löschung aus den Suchergebnissen ist ein erhöhtes Interesse der betroffenen Person gegenüber dem öffentlichen Interesse an der Verfügbarkeit der Suchergebnisse. Google Inc. wägt die Datenschutzrechte des Antragstellers ab, indem geprüft wird, ob die Daten veraltet sind und ob ein öffentliches Interesse daran besteht, die Daten im Suchergebnis zu finden.

Weiters ist ein Identitätsnachweis zu erbringen, der im elektronischen Formular als digitale Kopie abgesendet werden kann.

Google bietet auf seiner Website ein Online-Formular an, mit dem unter Angabe der oben genannten Voraussetzungen und Nennung der personenbezogenen Daten, also den in der Suchanfrage verwendeten Namen, sowie der URL der Ergebnisliste ein Antrag auf Entfernen von Suchergebnissen nach europäischem Datenschutzrecht gestellt werden kann. Alternativ kann die Zustellung auch per Mail, per Fax oder per Brief eingebracht werden.

5.1.2 Löschung der Daten aus Sicht von Google


---

Seit Einführung des neuen Verfahrens am 29. Mai 2014 wurden insgesamt 1.287.125 URLs überprüft, wobei mit 57,8 % mehr als die Hälfte der Links tatsächlich gelöscht werden mussten.


5.2 Lösung im Unternehmensbereich

Die Durchsetzung des Rechts auf Lösung im privatwirtschaftlichen Bereich stellt sich mitunter als schwieriger dar als im öffentlichen Bereich. Gerade private Unternehmen haben ein großes Interesse an möglichst vielen Daten, da ein großer Vorrat von Daten mit hohem Gewinn gleichgesetzt werden kann. So sollen beispielsweise einmal akquirierte Daten und Datensätze, wenn möglich, nicht so schnell wieder gelöscht werden.

Spezielle Probleme können sich dabei ergeben, wenn die Daten missbräuchlich iSd UWG oder des UrhG verwendet werden, da im Internet gerade durch Suchmaschinen die unrechtmäßig verwendeten Daten schnell verbreitet werden können. Folgend werden nur einige wenige Beispiele mit hoher praktischer Relevanz erläutert.

5.2.1 Urheberrechtliche Aspekte von Inline-Links und Framing


Im Einzelfall ist aber die Ausgestaltung des Links und des Inhalts zu berücksichtigen und somit zwischen Hyperlinks und Inline-Links bzw Frames zu unterscheiden.

Hyperlinks verweisen auf eine fremde Website und dem Nutzer ist dabei klar ersichtlich, dass er die Quellseite verlässt und auf eine neue Zielseite gelangt.
Mithilfe von Inline-Links können Dateien, Grafiken, Videos etc in die Webseite eingebunden werden. Die einzubindende Datei liegt auf einem Server und wird durch Angabe der Adresse auf der Webseite angezeigt. Der Besucher erkennt am ersten Blick nicht, ob das Element vom eigenen oder einem fremden Server stammt und macht für ihn auch keinen Unterschied. Die Herkunft lässt sich nur mit Hilfe des Quelltextes oder durch Anzeige der Eigenschaften des Elements feststellen.123

Frames bieten hingegen die Möglichkeit, in einem Browserfenster gleichzeitig mehrere Webseiten darzustellen. Die gesamte Webseite wird dazu in einzelne Segmente (=Frames) geteilt und nebeneinander, übereinander oder verschachtelt angezeigt. So lassen sich ganze Webseiten von fremden Anbietern in die eigene Webseite integrieren. Für den Benutzer ist ebenso wie bei Inline-Links nicht sofort erkennbar, dass die Elemente nicht vom Linksetzer stammen.124

Werden nun auf der Webseite fremde Inhalte mittels Inline-Linking oder Framing eingebettet, stellt sich die Frage, ob hierfür eine konkludente Zustimmung des Urhebers vorliegt. Nach den allgemeinen zivilrechtlichen Regeln kann dies jedenfalls nur solange angenommen werden, als es keinen vernünftigen Grund, daran zu zweifeln, gibt.125

Der EuGH hat im Oktober 2014 dazu eine grundlegende Entscheidung126 gefällt, die eine Einbettung von fremden Inhalten wohl erheblich erleichtert. Demnach stellt die Einbettung eines geschützten und im Internet öffentlich zugänglichen Werkes für sich alleine gerade keine öffentliche Wiedergabe iSd Art 3 Abs 1 der Urheberrechts-Richtlinie dar, soweit das Werk weder für ein neues Publikum noch mit einem anderen technischen Verfahren wiedergegeben wird.

Problematisch wird dies aber, wenn Werbung angezeigt wird und der eingebettete Inhalt mit der fremden Werbung in Beziehung gesetzt wird. In einem derartigen Fall hat das LG Köln in der E 28 O 141/01 die konkludente Zustimmung zu Frame-Links jedenfalls abgelehnt.

### 5.2.2 Wettbewerbsrechtlicher Schutz von Kennzeichen, Marken und Domains

Im wirtschaftlichen Bereich existiert ein allgemeiner Schutz gegen den unlauteren Wettbewerb iSd UWG. Die § 1 UWG (Generalklausel), § 2 UWG (Irreführung) sowie § 9 UWG

---

123 Ott, Urheber- und wettbewerbsrechtliche Probleme von Linking und Framing (2004), 49.
124 Stomper, Urheberrechtliche Aspekte von Links, ÖBl 2002/44.
125 Vgl § 863 ABGB.
Recht auf Löschung der Daten

(Missbrauch von Unternehmenskennzeichen) sind vor allem für Domainnamen zu berücksichtigen.

Voraussetzung ist hierbei immer ein Wettbewerbsverhältnis zwischen beiden Parteien. Beide müssen zumindest auf einem ähnlichen Gebiet tätig sein.\textsuperscript{127}

Irreführung ist immer dann anzunehmen, wenn mit Hilfe des Domain-Namens der Eindruck entstehen soll, dass es sich um eine andere Firma handelt. Aber auch der Fall des Typosquatting\textsuperscript{128} stellt eine Irreführung dar. Durch Typosquatting werden ähnlich klingende Domain-Namen meist mit oft vorkommenden Tippfehlern oder fehlerhafter Schreibweise verwendet, um den Anschein zu erwecken, es bestünde eine Verbindung zu einer bekannten Firma.\textsuperscript{129} Sofern dem Besucher nicht unmittelbar erkennbar ist, dass er auf der „falschen“ Webseite gelandet ist, stellt dies einen Verstoß gegen §§ 1 und 2 UWG dar.

Für diese Fälle gibt es ein spezielles Streitbeilegungsverfahren der ICANN\textsuperscript{130}, das von allen Registrierungsstellen für gTLDs und verschiedenen ccTLD-Registrierungsstellen angewandt wird. Zwischen 2000 und 2010 wurden mehr als 17.000 Fälle nach diesem UDRP-Verfahren (=Uniform Domain-Name Dispute-Resolution Policy) entschieden.\textsuperscript{131} Der Beschwerdeführer muss dabei nachweisen, dass

1. der Domain-Name identisch oder verwechslungsfähig ähnlich ist,
2. der Domain-Inhaber weder das Recht noch ein berechtigtes Interesse hinsichtlich des Namens besitzt,
3. der Domain-Name bösgläubig registriert wurde,
4. der Domain-Name bösgläubig verwendet wird.

Als Rechtsfolge kommt ausschließlich die Löschung bzw der Transfer des Domain-Namens in Frage. In der Praxis wird immer nur ein Transfer verlangt, da durch die Löschung jeder Dritte in der Zwischenzeit den Domain-Namen erneut registrieren könnte.\textsuperscript{132}

\textsuperscript{127} Sonntag, Einführung in das Internetrecht\textsuperscript{2} (2014), 25.
\textsuperscript{128} Vgl Seidelberger, Wettbewerbsrecht und Internet, RdW 2000/500.
\textsuperscript{130} Die Internet Coporation for Assigned Names and Numbers koordiniert die Vergabe von einmaligen Namen und Adressen im Internet.
\textsuperscript{131} Fuchs, Alternative dispute resolution according to the WIPO Uniform Domain name Dispute Resolution Policy (UDRP), Jahrbuch International Arbitration 2010, 305.
\textsuperscript{132} Sonntag, Einführung in das Internetrecht\textsuperscript{2} (2014), 48.
5.2.3 Mitarbeiterdaten

Die Verarbeitung von Arbeitnehmerdaten ist nicht nur für die betriebliche Datenverarbeitung, sondern auch für Arbeitnehmervertreter, Personal- und IT-Abteilung von hoher Relevanz. Neben datenschutzrechtlichen Aspekten wirft diese Thematik auch arbeitsverfassungsrechtliche Fragen auf, die meist in Betriebsvereinbarungen geregelt werden.

Von den in § 96 Abs 1 ArbVG genannten zustimmungspflichtigen Maßnahmen sind vor allem die Einführung von Personalfragebögen (Z 2) und die Einführung von Kontrollmaßnahmen (Z 3) datenschutzrechtlich äußerst relevant.

**Personalfragebögen** sind Maßnahmen, die geeignet sind, dem Arbeitgeber Informationen über Meinungen oder persönliche Umstände des Arbeitnehmers zu verschaffen, an denen der einzelne Arbeitnehmer ein Interesse an deren Geheimhaltung haben könnte. Eine Zustimmungspflicht ist aber entbehrlich, sofern die Befragung anonym abgehalten wird oder die Auswertung nicht einem Arbeitnehmer zugeordnet werden kann.\(^{133}\)

**Kontrollmaßnahmen und technische Systeme** ermöglichen eine systematische Überwachung der Arbeitnehmer durch den Betriebsinhaber. Dies kann zB durch Zutrittskontrollen erfolgen, um den Zeitpunkt des Betretens oder Verlassens des Betriebes festzustellen, oder aber auch Überwachungsmaßnahmen, die überhaupt den gesamten Aufenthalt im Betrieb zu einem beliebigen Zweck aufzeichnen, wie beispielsweise Videoüberwachung.\(^{134}\) Geeignete Kontrollmaßnahmen sind neben der Videoüberwachung auch die elektronische Zeiterfassung, Anwesenheitskontrolle, Telefonüberwachung, etc.\(^{135}\)

In einer Betriebsvereinbarung sollte jedenfalls das zulässige Ausmaß der Datenverarbeitung geregelt sein, sowie die Übermittlungsarten und allfällige Dienstleistungen angeführt werden, damit der Betriebsrat entsprechende Mechanismen für eine effektive Kontrolle des Systems vorsehen kann.\(^{136}\)

Ein weiteres Spannungsfeld zwischen Arbeitnehmer und Betriebsinhaber kann sich aus der Kontrolle von E-Mail und Internetnutzung am Arbeitsplatz ergeben. Die private Nutzung von E-Mails und Internet **ist** gesetzlich nicht geregelt und bedarf einer innerbetrieblichen Regelung. Der Arbeitnehmer hat grundsätzlich kein generelles Recht auf private Nutzung von E-Mail und Internet am Arbeitsplatz.\(^{137}\) Die Kontrolle der E-Mail- und Internetnutzung ist


\(^{135}\) Knyrim, Datenschutzrecht\(^3\) (2015), 247.

\(^{136}\) Knyrim, Datenschutzrecht\(^3\) (2015), 253.

\(^{137}\) Thiele, Internet am Arbeitsplatz – Erste arbeitsrechtliche Konfliktfälle, ecolex 2001, 613.
hinsichtlich der Protokollierung von Verbindungsdaten bei einem Verbot der Privatnutzung grds unproblematisch, wenn nur jene Daten protokolliert werden, die für die Aufrechterhaltung des IT-Systems unbedingt notwendig sind.

Aber auch bei einem generellen Verbot der Privatnutzung ist eine uneingeschränkte Überwachung unzulässig. Der Einsatz einer speziellen Überwachungssoftware zur Protokollierung des Nutzungsverhaltens des Arbeitnehmers im Internet würde regelmäßig die Menschenwürde verletzen und unzulässig sein.


5.3 Löschung im Privatbereich

Im Privatbereich gibt es gerade im Bereich der Social-Media-Plattformen vermehrt datenschutzrechtliche Bedenken.


Facebook ist mit mehr als 1,06 Mrd registrierten Nutzern die weltweit größte und bedeutendste Social-Media-Plattform. Nach Angaben des Social Media Radar Austria sind etwa 3,4 Mio Österreicher registriert.

---

139 Knyrim, Datenschutzrecht³ (2015), 267.
141 Klein in Splittgerber, Praxishandbuch Rechtsfragen Social Media, Kap 1 Rn 1.
142 Walther, Die Zulässigkeit der Datenverwendung als Voraussetzung des Rechts auf Löschung, 57.
144 Social Media Radar Austria ist ein Dienst der Social Media Agentur Digital Affairs. Die Daten werden laufend aktualisiert und sind direkt mit Facebook verknüpft.
Sind die Daten in einem sozialen Netzwerk zwar personenbezogen, aber allgemein verfügbar und öffentlich zugänglich, so verliert der Nutzer den Schutz auf Geheimhaltung seiner Daten. Wurden die Daten rechtmäßig und zulässigerweise veröffentlicht, und sind sie somit für jedermann auffindbar, sind die Daten allgemein verfügbar.\textsuperscript{145} Beispielsweise sind Profilbild und Name des Profils solche allgemein verfügbaren Daten, die nicht dem Schutz auf Geheimhaltung unterliegen, sofern die Privatsphäre-Einstellungen nicht entsprechend gewartet werden.\textsuperscript{146}

\textsuperscript{145} Jahnel, Datenschutzrecht (2014), Rz 2/18.
\textsuperscript{146} Walther, Die Zulässigkeit der Datenverwendung als Voraussetzung des Rechts auf Löschung (2015), 58.
6 KONKLUSION


Zusammenfassend kann festgehalten werden, dass es zwar uU Möglichkeiten zu partiellen Lösungen im Internet gibt, ein gesetzliches Recht auf Vergessen aber deswegen nicht besteht.

Im Zweifel kann davon ausgegangen werden, dass das Internet nichts vergisst!
**Literaturverzeichnis**


*Dohr/Pollirer/Weiss/Knyrim*, DSG² (2014)

*Fuchs*, Alternative Dispute Resolution according to the WIPO Uniform Domain Name Dispute Resolution Policy (UDRP), (2010)

*Gaderer* in *Kucsko*, urheber.recht (2007)


*Graf*, Datenschutzrecht im Überblick² (2010)


*Grünanger/Goricnik*, Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle (2014)

*Handig*, Das Zurverfügungstellungsgesetz und die Hyperlinks ecolex 2004/38

*Hengstschläger/Leeb*, Grundrechte² (2013)

*Jahnel*, Jahrbuch Datenschutzrecht (2014)

*Jahnel*, Lösungspflicht von Suchmaschinenbetreibern Die „Google Spain und Google“-Entscheidung des EuGH, jusIT 2014/72, 149

*Jahnel/Thiele*, Datenschutz durch Wettbewerbsrecht, ÖJZ 2004/55

*Klein in Splittergerber*, Praxishandbuch Rechtsfragen Social Media (2014)

*Knyrim*, Datenschutzrecht³ (2015)


*Kotschy/Reimer*, Die Überwachung der Internet-Kommunikation am Arbeitsplatz, ein Diskussionsbeitrag aus datenschutzrechtlicher Sicht, ZAS 2004/29
Leiter, Der Datenschutzbeauftragte – Theorie und Praxis, ZIR 2014/13


Plöckinger/Duursma/Mayrhofer, Internet-Recht (2004)

Pollirer, Die Datenschutz-Grundverordnung: Der Datenschutzbeauftrage, Dako 2015, 65


Seidelberger, Wettbewerbsrecht und Internet, RdW 2000/500

Skopik, Cyber Attack Information System (2015)

Sonntag, Einführung in das Internetrecht (2014)

Stessl, Internetsuchmaschinen und Datenschutz (2008)

Stomper, Urheberrechtliche Aspekte von Links, ÖBI 2002/44

Thiele, Internet am Arbeitsplatz – Erste arbeitsrechtliche Konfliktfälle (2001)

Unger, Grundzüge des Datenschutzrechts (2015)


Zankl, E-Commerce-Gesetz in Sicht, AnwBl 2001/459