Anwendbarkeit der EU-Datenschutzgesetzgebung auf Behörden, Einrichtungen und sonstige Stellen des Kantons Basel-Stadt

Inhaltsübersicht: ***(v1.0, Stand: 12.10.2018)***

1 Allgemeine Ausführungen

Die EU-Datenschutzgesetzgebung ist am 25. Mai 2018 in Kraft getreten. Sie besteht zurzeit[1] insbesondere aus der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (**Datenschutz-Grundverordnung**)[2] (abgekürzt: DSGVO).

Auf 2020 wird ein zweiter Erlass, der insbesondere die elektronische Kommunikation, die elektronische Werbung sowie das Internet-Tracking regelt, in Kraft treten, nämlich der **Vorschlag** vom 10. Januar 2017 für eine Verordnung des europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) (**Verordnung über Privatsphäre und elektronische Kommunikation**)[3].

Die EU-Datenschutzgesetzgebung gilt in erster Linie für Datenverarbeitungen innerhalb der EU. Sie enthält jedoch Normen, die dazu führen, dass auch Datenverarbeitungen durch Institutionen, die ihren Sitz ausserhalb der EU haben (z.B. in der Schweiz), unter die EU-Datenschutzgesetzgebung fallen. Fällt eine Datenverarbeitung in den Anwendungsbereich der EU-Datenschutzge-

1 Neben der am gleichen Tag in Kraft getretenen, für die justizielle und polizeiliche Zusammenarbeit geltenden Richtlinie (EU) 2016/680, ABl L 119 vom 4.5.2016, S. 89–131.
2 ABl L 119 vom 4.5.2016, S. 1-88.
3 COM(2017) 10 final.

setzgebung, spielt es keine Rolle, ob diese durch eine natürliche oder juristische Person des Privatrechts oder durch Behörden jeglicher Hierarchiestufen erfolgt (in der Schweiz: Bund, Kantone oder Gemeinden). Die EU-Datenschutzgesetzgebung ist in diesem Fall stets anwendbar.

Die nachfolgenden Ausführungen zeigen auf, was aus Sicht von Behörden, Einrichtungen oder anderen Stellen mit Blick auf eine mögliche Anwendbarkeit der EU-Datenschutzgesetzgebung zu beachten ist.

Anzumerken ist, dass die Reichweite vieler DSGVO-Regelungen noch nicht geklärt ist. Mehr Klarheit wird erst die Auslegung durch die Aufsichtsbehörden in der EU und schliesslich durch den Europäischen Gerichtshof (EuGH) bringen. Die folgenden Ausführungen erfolgen unter dem entsprechenden Vorbehalt.

2 Persönlicher Anwendungsbereich

Die EU-Datenschutzgesetzgebung gilt in persönlicher Hinsicht für jene Person oder Institution, die für die Datenbearbeitung verantwortlich ist. Nach Art. 4 Ziff. 7 DSGVO ist ein Verantwortlicher jene 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.

Die EU-Datenschutzgesetzgebung definiert dabei weder den Begriff der juristischen Person noch jenen der Behörden, Einrichtungen oder anderen Stellen. Während allgemeines Praxis entspricht, dass sich der Begriff der juristischen Personen nach dem massgeblichen nationalen Recht richtet, kam im Rahmen der neuen EU-Datenschutzgesetzgebung die Frage auf, wie es sich mit dem Begriff der Behörden, Einrichtungen und anderen Stellen verhält. Die Artikel-29-Datenschutzgruppe[4] hat sich dazu in einer Stellungnahme dahingehend geäussert, dass sich diese Begriffe nach dem jeweiligen nationalen Recht bestimmen sollten.[5] Diese Vorgehensweise erscheint zielführend. Es gibt keinen Grund, weshalb sich der Begriff der juristischen Personen nach dem nationalen Recht bestimmen soll, jener der Behörden, Einrichtungen und anderen Stellen dagegen nicht. Zudem kennen die verschiedenen Länder teilweise unterschiedliche Behördenformen und Einrichtungen, die sich nicht ohne weiteres unter eine von der EU vorgegebene Definition subsumieren lassen. Für diese Interpretation spricht auch das Vorgehen von Deutschland. Deutschland definiert in seinem an die EU-Datenschutzgesetzgebung angepassten neuen Bundesdatenschutzgesetz (BDSG) unter den Begriffsbestimmungen (§ 2 BDSG) lediglich noch die Behörden, Einrichtungen und anderen Stellen. Für alle anderen Begriffsbestimmungen verweist dieses auf Art. 4 DSGVO. Für die Schweiz würde das somit bedeuten, dass sich der Begriff der Behörden, Einrichtungen und sonstigen Stellen des Bundes nach dem DSG/Bund und jener der kantonalen Behörden, Einrichtungen und sonstigen Stellen nach dem jeweils anwendbaren kantonalen (Informations- und) Datenschutzgesetz bestimmen.

---

4 Die Artikel-29-Datenschutzgruppe wurde nach Art. 29 der Richtlinie 95/46/EG eingesetzt. Sie ist ein unabhängiges Beratungsgremium der EU zum Themenkreis Datenschutz und Schutz der Privatsphäre. Sie wird unter der neuen EU-Datenschutzgesetzgebung durch den Europäischen Datenschutzausschuss nach Art. 68 DSGVO ersetzt.

5 ARTIKEL-29-DATENSCHUTZGRUPPE, Leitlinien in Bezug auf Datenschutzbeauftragte (DSB), angenommen am 13.12.2016, Stand 5.4.2017, S. 6 f., abrufbar über die Webseite des Hamburgischen Datenschutzbeauftragten: https://datenschutz-hamburg.de/assets/pdf/wp243rev01_de.pdf.

3 Räumlicher Anwendungsbereich

Es gibt drei Bereiche, in denen die EU-Datenschutzgesetzgebung für Behörden und Unternehmen in der Schweiz anwendbar ist (extraterritorial Anwendung findet):

- wenn die Behörde oder das Unternehmen über eine Niederlassung in der EU verfügt (3.1), oder
- wenn eine Behörde oder ein Unternehmen in der Schweiz Personen in der EU Waren oder Dienstleistungen anbietet (3.2) oder
- wenn Personen, die sich in der EU befinden, beim Besuch der Internetseite einer Behörde oder eines Unternehmens in der Schweiz mittels Analyse-Tools beobachtet werden (3.3).

3.1 Niederlassung in EU

Nach der EU-Datenschutzgesetzgebung liegt eine **Niederlassung** vor, wenn in der EU eine *feste Einrichtung* besteht, von der aus eine *Tätigkeit effektiv und tatsächlich stattfindet*.

3.1.1 Feste Einrichtung

Eine **feste Einrichtung** liegt vor, wenn sie einen gewissen Grad an Beständigkeit hat; mobile Geschäftsstätten oder Messestände sind keine festen Einrichtungen.

3.1.2 Effektiv und tatsächlich stattfindende Tätigkeit

Eine **effektiv und tatsächlich stattfindende Tätigkeit** erfordert irgendwie geartete menschliche Aktivitäten; Serverstandorte oder Briefkastenfirmen erfüllen diese Voraussetzung nicht.

Nur wenn beide Voraussetzungen erfüllt sind, liegt eine Niederlassung i.S. der EU-Datenschutzgesetzgebung vor. Ob die Niederlassung eigene Rechtspersönlichkeit hat, spielt keine Rolle.

Während bei Unternehmen Niederlassungen in einem EU-Staat problemlos denkbar sind, wird es kaum Behörden geben, die in einem EU-Staat eine Niederlassung haben (ausser diplomatische Dienste). Bei Einrichtungen und anderen Stellen sind dagegen Niederlassungen in einem EU-Mitgliedstaaten durchaus denkbar.

3.2 Anbieten von Waren und Dienstleistungen an Personen in der EU

Dieser Fall liegt vor, wenn eine schweizerische Behörde oder ein Unternehmen mit Sitz in der Schweiz *Waren oder Dienstleistungen* (3.2.1) *Personen in der EU anbietet* und dazu Personendaten über Personen in der EU bearbeitet (3.2.2):

3.2.1 Anbieten von Waren oder Dienstleistungen

Was unter Waren und Dienstleistungen zu verstehen ist, definiert die EU-Datenschutzgesetzgebung nicht.

Waren lassen sich jedoch unter Einbezug anderweitiger EU-Gesetzgebung definieren als alle beweglichen körperlichen Gegenstände, die einen Geldwert haben und Gegenstand von Handelsgeschäften sein können. Darunter fallen neben herkömmlichen Handelswaren auch Energieträger (Öl, Gas, Strom), Saatgut, Tiere, Abfälle, Kunstgegenstände oder Träger immaterieller Güter (z.B. Ton- und Bildträger).

Der Begriff der **Dienstleistungen** ist nach Ansicht der Literatur weit zu verstehen. Eine Dienstleistung stellt eine Teilnahme am Wirtschaftsleben dar, wird in der Regel gegen Entgelt[6] erbracht und ist auf ein Bedürfnis des Kunden ausgerichtet. Darunter fallen insbesondere auch jede Art von Internet-Dienstleistungen wie z.B. im Internet buchbare Reisen, Cloud-Angebote, das Anbieten von Apps, Social Media-Angebote oder Streaming-Dienste. Im behördlichen Umfeld ist jedoch davon auszugehen, dass hoheitliches Handeln des Staates, das Verwaltungsakte wie z.B. Bewilligungen und/oder Verfügungen hervorbringt, keine Dienstleistung i.S. der EU-Datenschutzgesetzgebung darstellt, auch wenn die Adressaten der Verwaltungsakte Personen in der EU sind. Hoheitliches Handeln des Staates ist keine Teilnahme am Wirtschaftsleben; das gilt nach der EU-Rechtsprechung auch bei Leistungen, die vollständig oder überwiegend durch öffentliche Abgaben (d.h. mit Steuergeldern) finanziert werden. Ebenfalls keine Dienstleistungen i.S. der EU-Datenschutzgesetzgebung dürften Leistungen darstellen, die ein Staat gestützt auf ein staatsvertragliches Abkommen für einen anderen Staat erbringt, z.B. in Grenzkantonen im Bereich von Schutz und Rettung. Anders verhält es sich, wenn der Staat als gleichberechtigter Marktteilnehmer auftritt und damit im Wettbewerb zu anderen Marktteilnehmern steht. In diesem Bereich kann auch eine Behörde Dienstleistungen i.S. der EU-Datenschutzgesetzgebung erbringen.

3.2.2 Anbieten an Personen in der EU

Ein Angebot geht an **Personen in der EU**, wenn diese sich *zum Zeitpunkt der fraglichen Datenbearbeitung* in der EU befinden. Die Staatsangehörigkeit spielt keine Rolle.

Klarerweise zielt z.B. das Schalten von Werbung in Zeitungen, Radio- und Fernsehstationen oder Suchmaschinen in der EU oder das Verteilen von Werbematerial in EU-Staaten darauf ab, Personen in der EU etwas **anzubieten**. Für das Anbieten ist aber nicht zwingend ein aktives Handeln der anbietenden Institution notwendig. Auch das passive Bereithalten eines Angebots kann ein Angebot i.S. der EU-Datenschutzgesetzgebung darstellen. Allerdings ist davon auszugehen, dass das blosse Zugänglichmachen einer Webseite in der EU kein Angebot i.S. der EU-Datenschutzgesetzgebung darstellt. Es braucht eine *Kombination zusätzlicher Elemente* wie z.B. Angebote in Euro und/oder in EU-länderspezifischen Sprachen (in der Schweiz ist die Verwendung der eigenen Landessprachen Deutsch, Französisch und Italienisch allerdings kein Indiz), neutrale Domainnamen wie .eu oder .com, Domainnamen mit Top-Level-Domains von anderen Ländern als denjenigen, wo die Behörde oder das Unternehmen seinen Sitz oder eine Niederlassung hat (nicht .ch, sondern z.B. .de, .pl), Wegbeschreibungen aus dem Ausland zum Waren- oder Dienstleistungsort, das Aufführen von Kundenbewertungen von Kunden in der EU usw.

---

[6] Die DSGVO sieht vor, dass auch das Anbieten unentgeltlich erbrachter Dienstleistungen zur Anwendung des EU-Datenschutzrechts führen kann. Abgezielt wurde damit auf Internet-Weltkonzerne wie Facebook oder Twitter. Bei Lichte betrachtet erbringen sie ihre Dienstleistungen nicht unentgeltlich: Bezahlt wird mit Daten, die sie dann kommerziell nutzen.

Insgesamt ist festzuhalten, dass die Beurteilung, inwiefern ein Anbieten stattfindet, jedenfalls nur einzelfallbezogen und zurzeit in vielen Fällen nicht abschliessend möglich ist. Dies wird erst möglich sein, wenn der Europäische Datenschutzausschuss nach Art. 68 DSGVO eine entsprechende Praxis entwickelt hat und/oder zu dieser Frage Gerichtsentscheide ergangen sind. Ist von einem Anbieten i.S. der DSGVO auszugehen, lässt sich zudem fragen, ob dem Ort, an dem die Dienstleistung erbracht wird, wie in Kommentaren angetönt, tatsächlich keine Bedeutung zukommt. Insbesondere in Fällen, in denen die Dienstleistung ausschliesslich oder hauptsächlich ausserhalb der EU erbracht wird, stellt sich die Frage, ob die Anwendbarkeit der EU-Datenschutzgesetzgebung wirklich zielführend ist. Zurzeit ist diese Frage allerdings unbeantwortet.

3.3 Verhaltensbeobachtung (Tracking und Profiling) in der EU

Die EU-Datenschutzgesetzgebung findet Anwendung, wenn eine Institution mit Sitz in der Schweiz Daten über natürliche Personen verarbeitet, um das *Verhalten dieser Personen zu beobachten* (4.1), sofern *das Verhalten in der EU stattfindet* (4.2).

3.3.1 Beobachtung des Verhaltens von Personen

Diese Regelung bezieht sich ausschliesslich auf Datenverarbeitungen, die dem **Beobachten der Internetaktivitäten einer natürlichen Person** dienen (Tracking) – inklusive der Verwendung von Techniken zur Erstellung eines Profils der betroffenen Person, anhand dessen sich deren Vorlieben oder Verhaltensweisen analysieren oder voraussagen lassen (Profiling). Damit ein Beobachten vorliegt, muss dieses eine bestimmte Dauer und eine gewisse Intensität aufweisen. Insbesondere der Einsatz von Analyse-Tools wie Cookies oder Social Plugins (z.B. Like-Button von Facebook) sowie der Einsatz von Value-Added Services (Mehrwertdienste, die Basisdienste individuell ergänzen) führen stets zum Vorliegen eines Beobachtens i.S. der EU-Datenschutzgesetzgebung.

Mit Blick auf Webseiten, die Tracking-und Profiling-Tools verwenden, ist davon auszugehen, dass es für ein Beobachten i.S. der EU-Datenschutzgesetzgebung nicht darauf ankommt, ob sich die Webseite gezielt an Personen in der EU wendet (anders als beim Anbieten von Waren und Dienstleistungen, oben 3.2). Damit wird jeder Webseitenanbieter, der entsprechende Tools einsetzt, von der EU-Datenschutzgesetzgebung erfasst, sofern sich die Nutzer (auch Schweizer oder US-Amerikaner) im Zeitpunkt des Besuchs der Webseite in der EU befinden und die eingesetzten Tracking- und Profiling-Tools zu einer Verarbeitung personenbezogener Daten führen.

Festzuhalten ist, dass der Datenschutzbeauftragte des Kantons Basel-Stadt schon vor geraumer Zeit darauf aufmerksam gemacht hat, dass es für einen (über die IP-Adresse identifizierenden) Einsatz von Tracking- oder Profiling-Tools (z.B. Google Analytics) durch öffentliche Organe des Kantons Basel-Stadt nach schweizerischem Recht keine gesetzliche Grundlage gibt.

3.3.2 Verhalten in der EU

Das **Verhalten** erfolgt **in der EU**, wenn sich die von der Beobachtung betroffenen Personen während der Nutzung des Internets physisch innerhalb der EU befinden. Dies lässt sich jeweils anhand der IP-Adresse des Endgeräts der betroffenen Person feststellen.

Behörden sollten daher prüfen, inwiefern im Rahmen ihrer Webseite der Einsatz von Tracking- und Profiling-Instrumenten stattfindet. Ein entsprechender Einsatz könnte zur Anwendbarkeit der EU-Datenschutzgesetzgebung führen. Erfolgt ein entsprechender Einsatz, empfiehlt sich eine Prüfung, inwiefern der Verzicht auf Tracking- und Profiling-Instrumente möglich ist. Eine weitere Möglichkeit besteht darin, Besucher mit einer IP-Adresse aus dem EU-Raum mittels Geolokalisierungs-Tools vom Tracking und Profiling auszunehmen.

4 Wichtigste Vorgaben der EU-Datenschutzgesetzgebung

Ist die Anwendbarkeit der EU-Datenschutzgesetzgebung zu bejahen, untersteht nicht das gesamte Datenbearbeiten der Behörde, Einrichtung oder sonstigen Stelle der DSGVO, sondern nur die vom Anwendungsbereich erfasste Datenbearbeitung. Die Behörde, Einrichtung oder sonstige Stelle fällt somit nicht mit Blick auf alle Personendatenbearbeitungen unter die EU-Datenschutzgesetzgebung.

Auch ist bei der neuen EU-Datenschutzgesetzgebung keineswegs alles neu. Sie enthält über weite Strecken Regelungen, die schon im bisher geltenden Recht (für öffentliche Organe des Kantons Basel-Stadt: im Informations- und Datenschutzgesetz [IDG]) enthalten waren. Wenn eine Behörde, Einrichtung oder sonstigen Stelle das bisher geltende Datenschutzrecht konsequent umgesetzt hat, hat sie einen Grossteil der Arbeit schon gemacht. Oder wie es der Datenschutzverantwortliche eines Basler Weltkonzerns kürzlich gesagt hat: Den grössten Aufwand musste er nicht treiben wegen der neuen Regelungen in der DSGVO, sondern zur konsequenten Durchsetzung der bereits vorher geltenden Datenschutzbestimmungen – weil die Nichteinhaltung nun sanktioniert werden kann.

Die nachfolgende Tabelle enthält eine Übersicht über die wichtigsten Vorgaben der EU-Datenschutzgesetzgebung und zeigt auf, inwiefern diese auch durch das baselstädtische IDG abgedeckt sind bzw. bei dessen Anpassung an das europäische Datenschutzrecht umgesetzt werden sollen.

EU-Datenschutz-Grundverordnung (DSGVO)		**IDG/BS**	
Art.	Inhalt	§	Inhalt
4 Ziff. 11 i.V.m. Art. 7	**Einwilligung** Eine gültige Einwilligung liegt nur vor, wenn sie für den bestimmten Fall (den bestimmten Verwendungszweck), freiwillig (ohne Zwang), in informierter Weise und unmissverständlich (aus Beweisgründen schriftlich) erfolgte. *Anmerkung:* Insbesondere Einwilligungen, die als Opt-Out-Version ausgestaltet sind, erfüllen diese Anforderungen nicht. Bereits mit einem Häkchen versehene Boxen, z.B. zum Bestellen eines Newsletters, sind nicht mehr zulässig. Vielmehr müssen unter der DSGVO sämtliche Einwilligungen als Opt-In-Version ausgestaltet sein und die Boxen müssen von den Betroffenen aktiv mit einem Häkchen versehen werden.	21	Die Einwilligung ist nur bei der Bekanntgabe von Personendaten als Rechtfertigungsgrund vorgesehen (nicht beim Bearbeiten generell: vgl. PK-IDG/BS, § 9 N 42 ff.). Dabei wird schon heute ein Opt-in verlangt (vgl. PK-IDG/BS, § 21 N 24).

EU-Datenschutz-Grundverordnung (DSGVO)		IDG/BS	
Art.	Inhalt	§	Inhalt
13	**Informationspflicht bei der Datenerhebung** Werden personenbezogene Daten bei der betroffenen Person erhoben, teilt der Verantwortliche der betroffenen Person im Zeitpunkt der Datenerhebung den Namen und die Kontaktdaten des Verantwortlichen, die Zwecke der Datenverarbeitung sowie die Rechtsgrundlage für die Verarbeitung (nur wenn Verarbeitung nicht auf Einwilligung beruht) mit.	15 Abs. 3	Eine Informationspflicht ist bisher nur bei der Erhebung besonderer Personendaten vorgesehen, wird aber bei der Anpassung an das europäische Datenschutzrecht ausgeweitet werden müssen.
17	**Recht auf Löschung (Recht auf Vergessenwerden)** Die von der Datenverarbeitung betroffene Person hat das Recht, vom Verantwortlichen zu verlangen, dass dieser bei Vorliegen gewisser Umstände, alle Daten, die sich auf die betroffene Person beziehen, löscht.	---	Bisher keine Regelung. Ein solches Recht soll aber bei der Anpassung an das europäische Datenschutzrecht ins IDG aufgenommen werden.
20	**Recht auf Datenübertragbarkeit:** Die von einer Datenverarbeitung betroffene Person hat unter gewissen Umständen das Recht, sie betreffende personenbezogene Daten, die sie einem Verantwortlichen zur Verfügung gestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und diese Daten einem anderen Verantwortlichen zu übermitteln (Stichwort Wechsel von Providern).	---	Bisher keine Regelung. Es ist fraglich, ob das Recht bei der Anpassung an das europäische Datenschutzrecht für öffentliche Organe ins IDG aufgenommen werden muss, da es primär auf privatrechtliches Datenbearbeiten zugeschnitten ist.
22	**Automatisierte Einzelentscheidungen** Die betroffene Person hat das Recht, nicht einer ausschliesslich auf einer automatischen Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkungen entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt (mit Ausnahmen). Ist ausnahmsweise eine automatisierte Einzelentscheidung zulässig, trifft der Verantwortliche angemessene Massnahmen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört.	---	Bisher keine Regelung. Es ist fraglich, ob die Regelung bei der Anpassung an das europäische Datenschutzrecht für öffentliche Organe ins IDG aufgenommen werden muss: Transparenz und Einwirkungsmöglichkeit sind bei Verwaltungsverfahren (Entscheid per Verfügung, rechtliches Gehör) in der Regel bereits gegeben.

EU-Datenschutz-Grundverordnung (DSGVO)		IDG/BS	
Art.	Inhalt	§	Inhalt
25 Abs. 1	**Privacy by Design** Bei der Implementierung und Ausgestaltung technischer und organisatorischer Massnahmen hat der Verantwortliche darauf zu achten, dass er die Datenschutzgrundsätze gemäss dem Stand der Technik wirksam umsetzt und deren Ausgestaltung mit der EU-Datenschutzgesetzgebung konform ist.	14	Teilweise bereits vorhanden. Privacy by Design als Grundsatz soll bei der Anpassung an das europäische Datenschutzrecht ins IDG aufgenommen werden.
25 Abs. 2	**Privacy by Default** Der Verantwortliche trifft geeignete technische und organisatorische Massnahmen, die sicherstellen, dass bei Voreinstellungen stets die datenschutzfreundlichste Variante zur Anwendung gelangt. – z.B. in Bezug auf die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, die Speicherfrist oder die Zugänglichkeit.	14	Teilweise bereits vorhanden. Privacy by Default als Grundsatz soll bei der Anpassung an das europäische Datenschutzrecht ins IDG aufgenommen werden.
27	**Vertretung in der Union** Findet die EU-Datenschutzgesetzgebung gestützt auf den Umstand, dass eine Niederlassung in der EU besteht, Personen in der EU Waren oder Dienstleistungen angeboten werden oder Personen beim Besuch einer Webseite beobachtet werden, Anwendung, muss der für die Datenverarbeitung Verantwortliche eine Vertretung in der EU bestimmen. *Anmerkung:* Diese Regelung gilt nicht für Behörden und öffentliche Stellen, selbst wenn die EU-Datenschutzgesetzgebung auf diese anwendbar ist.	---	
30	**Verzeichnis von Verarbeitungstätigkeiten** Jeder Verantwortliche führt ein Verzeichnis aller Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen.	24	Entspricht ungefähr dem Verzeichnis der Verfahren, bei denen Personendaten bearbeitet werden.
33	**Meldung von Datenschutzverletzungen (Data Breach Notification)** Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche diese unverzüglich der Aufsichtsbehörde, es sei denn, dass die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.	---	Die Meldepflicht bei Datenschutzverletzungen soll bei der Anpassung an das europäische Datenschutzrecht ins IDG aufgenommen werden.

EU-Datenschutz-Grundverordnung (DSGVO)		IDG/BS	
Art.	Inhalt	§	Inhalt
34	**Benachrichtigung der von einer Datenschutzverletzung betroffenen Person (Data Breach Notification)** Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung (mit Ausnahmen).	---	Die Meldepflicht bei Datenschutzverletzungen soll bei der Anpassung an das europäische Datenschutzrecht ins IDG aufgenommen werden.
35	**Datenschutz-Folgeabschätzung** Führt eine Verarbeitung personenbezogener Daten, insbesondere bei der Verwendung neuer Technologien, aufgrund der Art, des Umstands und der Zwecke der Verarbeitung voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen, muss der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchführen.	(13)	Bisher keine ausdrückliche Regelung, entspricht aber der Vorbereitung für die Einreichung eines Vorhabens zur Vorabkontrolle (§ 13 IDG). Die DSFA soll bei der Anpassung an das europäische Datenschutzrecht ins IDG aufgenommen werden.
37 Abs. 1 und 3	**Benennung eines (betrieblichen) Datenschutzbeauftragten** Sofern gewisse Voraussetzungen erfüllt sind, muss der Verantwortliche einen internen Datenschutzbeauftragten ernennen, so z.B. wenn die Kerntätigkeit die Verarbeitung personenbezogener Daten umfasst, die aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche, regelmässige und systematische Überwachung der betroffenen Personen erforderlich macht oder wenn die Kerntätigkeit die umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten umfasst (Abs. 1). Behörden oder öffentliche Stellen können für mehrere Behörden oder Stellen unter Berücksichtigung ihrer Organisationsstruktur und ihrer Grösse einen gemeinsamen Datenschutzbeauftragten ernennen (Abs. 3).	---	Bisher keine Regelung. Grössere Dienststellen mit sensitiven Personendaten haben von sich aus Datenschutzverantwortliche bezeichnet. Es wird bei der Anpassung an das europäische Datenschutzrecht zu prüfen sein, inwiefern eine Pflicht zur Benennung (betrieblicher) Datenschutzbeauftragter (Datenschutzberater) ins IDG aufgenommen werden soll.
83	**Geldbussen** Die Datenschutzaufsichtsstellen von EU-Mitgliedstaaten haben das Recht, bei Verstössen gegen die EU-Datenschutzgesetzgebung hohe Geldbussen zu besprechen. Je nach Verstoss betragen diese bis zu EUR 10 bzw. 20 Mio. und bei Unternehmen bis zu 2 bzw. 4% des gesamten weltweit erzielten Jahresumsatzes des vergangenen Geschäftsjahres – je nachdem, welcher Betrag höher ist.	---	Keine Regelung. Es ist auch nicht vorgesehen, bei der Anpassung an das europäische Datenschutzrecht eine Bussenregelung ins IDG aufzunehmen.

Beilage: Anwendungsbeispiele