RUOSS VOGELE

# Entwurf des DSG im Vergleich mit der DSGVO (eine Übersicht)

## Bulletin 2/2019

Zürich, Januar 2019

## Management Summary

Der Entwurf des Datenschutzgesetzes („E-DSG“) soll 2019 im Parlament behandelt werden. Er lehnt sich zu einem wesentlichen Teil an die neue EU Datenschutz-Grundverordnung („DSGVO“) an. In diesem Bulletin werden die neuen datenschutzrechtlichen Pflichten nach E-DSG und DSGVO übersichtsmässig dargestellt und verglichen. Des Weiteren wird kurz besprochen, wie die neuen Pflichten praktisch umgesetzt werden können und welche Sanktionen bei einer Nichtumsetzung drohen. Schliesslich werden die räumlichen Geltungsbereiche des E-DSG und der DSGVO erläutert.

Dr. Alois Rimle
Rechtsanwalt, LL.M.

**Inhalt**



## Neue Pflichten

### Neue Pflichten nach DSGVO

Die neue EU Datenschutz-Grundverordnung von 2016 („DSGVO“) trat im Mai 2018 in Kraft. Sie ist direkt anwendbar und ersetzt die EU-Datenschutzrichtlinie 95/46/EG. Die DSGVO wird durch Umsetzungserlasse der einzelnen EU/EWR-Mitgliedstaaten

ergänzt, die sowohl präzisierende als auch ergänzende Normen enthalten. Dies gilt beispielsweise für das revidierte deutsche Bundesdatenschutzgesetz von 2017 („BDSG").

Die DSGVO enthält verschiedene neue Pflichten, die über die Anforderungen des gegenwärtigen Datenschutzgesetzes der Schweiz hinausgehen. Es handelt sich insbesondere um folgende Änderungen:

- *Profilierung:* Der Begriff der Profilierung wird eingeführt. Er betrifft die Bewertung einer Person hinsichtlich spezifischer Merkmale auf automatisierte Weise (Art. 4 Ziff. 4 DSGVO).
- *Pflichtinformationen:* Die Datenerhebung muss nicht mehr nur transparent erfolgen (Erkennbarkeit für betroffene Person). Neu sind verschiedene Pflichtinformationen mitzuteilen bzw. bekanntzugeben (Deklarationspflicht) (Art. 13 und 14 DSGVO).
- *Automatisierte Einzelentscheide:* Bei automatisierten Einzelentscheiden mit gewichtigen Folgen (z.B. bei Online-Krediten) besteht ein Recht auf „menschliches Gehör". Die betroffene Person muss informiert werden und es muss ihr die Möglichkeit eingeräumt werden, sich mit einem Menschen über den Entscheid zu unterhalten (Art. 22 DSGVO).
- *Auskunftsrecht:* Das Auskunftsrecht ist inhaltlich beschränkt. Es besteht ein Schutz vor Missbräuchen (Art. 15 und 23 DSGVO).
- *Einwilligung:* Einwilligungen müssen separat eingeholt werden und einen Hinweis auf die jederzeitige Widerrufbarkeit enthalten (Art. 7 DSGVO). Angaben in den AGB sind nicht ausreichend. Bei Kindern gelten besondere Vorschriften (Art. 8 DSGVO).
- *Recht auf Vergessen:* Eine betroffene Person hat das Recht, bei Vorliegen bestimmter Gründe vom Verantwortlichen zu verlangen, dass seine Daten unverzüglich gelöscht werden (Art. 17 DSGVO).
- *Rechtfertigung von Vertragsabschluss oder -abwicklung:* Es werden nicht nur Daten des Vertragspartners, sondern neu auch Daten von Personen erfasst, in deren Interesse ein Vertrag ist (Art. 6 DSGVO).
- *EU-Vertreter:* Ein Unternehmen ohne Niederlassung im EU/EWR-Raum muss einen Vertreter ernennen, es sei denn, die Bearbeitung erfolgt nur gelegentlich und birgt keine besonderen Risiken für die Rechte und Freiheiten natürlicher Personen (Art. 27 DSGVO). Der Vertreter ist mit hinreichenden Kompetenzen auszustatten, damit er seine Aufgabe als Anlaufstelle für die betroffenen Personen und die zuständige Aufsichtsbehörde wahrnehmen kann.
- *Verzeichnis:* Ein Unternehmen und gegebenenfalls sein Vertreter müssen ein Verzeichnis aller Bearbeitungstätigkeiten erstellen, die ihrer Zuständigkeit unterliegen (Art. 30 DSGVO).
- *Data Breach:* Ein Unternehmen muss sicherstellen, dass auftretende Verletzungen des Schutzes von Personendaten der Aufsichtsbehörde gemeldet (Art. 33 DSGVO) und betroffene Personen bei einem hohen Risiko von Auswirkungen benachrichtigt werden (Art. 34 DSGVO).
- *Folgeabschätzung:* Ein Unternehmen muss bei einem voraussichtlich hohen Risiko für die Rechte und Freiheiten natürlicher Personen Datenschutz-Folgeabschätzungen erstellen (*Privacy Impact Assessments*) und dabei allenfalls die Aufsichtsbehörde konsultieren (Art. 35 und 36 DSGVO);
- *Datenschutzbeauftragter:* Ein Unternehmer und ein Auftragsbearbeiter müssen unter Umständen einen betrieblichen Datenschutzbeauftragten ernennen (Art. 37-39 DSGVO).
- *Privacy by Design:* Ein Unternehmen muss datenschutzrechtliche Massnahmen der Technikgestaltung (z.B. Pseudonymisierung) ergreifen (Art. 25 DSGVO).
- *Privacy by Default:* Ein Unternehmen muss für datenschutzrechtliche Voreinstellungen sorgen (Art. 25 DSGVO).
- *Datentransfer-Verträge:* Es bestehen neue Vorgaben für Verträge mit Auftragsbearbeitern (z.B. Vetorecht von Kunden betreffend Subunternehmern; keine Datenexporte ohne Weisung oder Zustimmung des Kunden) (Art. 28 DSGVO). Die gemeinsam für die Bearbeitung Verantwortlichen müssen durch Vereinbarung festlegen, wer für was verantwortlich ist (Art. 26 DSGVO).
- *Übermittlung ins Ausland mit Datenschutzklausel im Vertrag:* Personendaten dürfen ins Ausland bekannt gegeben werden, wenn geeignete Datenschutzklauseln vereinbart werden (Art. 46 DSGVO).

- *Übermittlung an ausländische Behörden:* Eine Übermittlung an ausländische Behörden ist zulässig, sofern dies zur Geltendmachung, Ausübung, oder Verteidigung von Rechtsansprüchen erforderlich ist (Art. 49 DSGVO). Dabei sind die Bearbeitungsgrundsätze einzuhalten.
- *Einverständliche Übermittlung ins Ausland:* Eine betroffene Person kann ausdrücklich einwilligen, dass ihre Daten in ein Land ohne angemessenen Datenschutz exportiert werden (Art. 49 DSGVO).
- *Datenportabilität:* Die Service-Nutzer können die über sie erhobenen Daten in einem gängigen Format zur eigenen Verwendung erhalten (Art. 20 DSGVO).
- *Begehren betroffener Personen:* Es bestehen hinsichtlich der Begehren von betroffenen Personen (Auskunft, Berichtigung, Löschung, Widerspruch) Neuerungen für Dokumente und Prozesse (Art. 12 ff. DSGVO).
- *Datenspeicherung:* Personendaten müssen frühzeitig pseudonymisiert und dann auch gelöscht oder anonymisiert werden (vgl. Art. 5 und 32 DSGVO).
- *Rechenschaftspflicht:* Verantwortliche sind für die Einhaltung der Bearbeitungsgrundsätze verantwortlich und müssen die Einhaltung nachweisen können (Art. 5 DSGVO).

## Neue Pflichten nach E-DSG

Das Bundesgesetz über den Datenschutz wird gegenwärtig vollständig überarbeitet. Der Entwurf soll 2019 im Parlament behandelt werden („E-DSG"). Dementsprechend wird auch die Verordnung zum Bundesgesetz über den Datenschutz vollständig überarbeitet.

Das E-DSG enthält verschiedene neue Pflichten, die sich zu einem wesentlichen Teil an die neuen Pflichten nach DSGVO anlehnen. Unterstellungspflichtige Unternehmen müssen in Zukunft insbesondere folgende Änderungen beachten:

- *Personendaten*: Daten, die sich auf juristische Personen beziehen, gelten nicht mehr als Personendaten im datenschutzrechtlichen Sinn (Art. 4 E-DSG).
- *Besonders schützenswerte Personendaten*: Der Katalog wurde um genetische und biometrische Daten erweitert (Art. 4 E-DSG).
- *Profilierung*: Der Begriff der Profilierung ersetzt den Begriff des Persönlichkeitsprofils und betrifft die Bewertung einer Person hinsichtlich spezifischer Merkmale auf automatisierte Weise (Art. 4 E-DSG).
- *Pflichtinformationen:* Die Datenerhebung muss nicht mehr nur transparent erfolgen (Erkennbarkeit für betroffene Personen). Neu sind verschiedene Pflichtinformationen mitzuteilen bzw. bekanntzugeben (Deklarationspflicht) (Art. 17 und 18 E-DSG).
- *Automatisierte Einzelentscheide:* Bei automatisierten Einzelentscheiden mit gewichtigen Folgen (z.B. bei Online-Krediten) besteht ein Recht auf „menschliches Gehör". Die betroffene Person muss informiert werden und es muss ihr die Möglichkeit eingeräumt werden, sich mit einem Menschen über den Entscheid zu unterhalten. Die betroffene Person kann ausdrücklich einwilligen und damit auf das Recht auf „menschliches Gehör" verzichten (Art. 19 E-DSG).
- *Auskunftsrecht:* Es besteht ein Auskunftsrecht mit erweitertem Inhalt. Dabei besteht wenig Missbrauchsschutz (Art. 23-25 E-DSG).
- *Einwilligung:* Die Anforderungen an eine gültige Einwilligung gehen weniger weit als nach der DSGVO. Die Rechtslage in der Schweiz bleibt grundsätzlich unverändert (Art. 5 E-DSG).
- *Recht auf Vergessen:* Eine betroffene Person kann vom Verantwortlichen verlangen, dass seine Daten unverzüglich gelöscht werden. Vorbehalten bleibt ein bestehender Rechtfertigungsgrund für die betreffende Datenbearbeitung (Art. 26 E-DSG).
- *Rechtfertigung von Vertragsabschluss oder -abwicklung:* Es werden nicht nur Daten des Vertragspartners, sondern neu auch Daten von Personen erfasst, in deren Interesse ein Vertrag ist (Art. 14 E-DSG).
- *Verzeichnis:* Es besteht eine Inventarpflicht. Der Verantwortliche und der Auftragsbearbeiter führen ein Verzeichnis ihrer Bearbeitungstätigkeiten (Art. 11 E-DSG).
- *Data Breach:* Ein Unternehmen muss sicherstellen, dass dem EDÖB auftretende Verletzungen der Datensicherheit gemeldet und betroffene Personen informiert werden, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt (Art. 22 E-DSG).
- *Folgeabschätzung:* Ein Unternehmen muss vorgängig eine Folgeabschätzung erstellen, wenn

eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann (*Privacy Impact Assessments*), und dabei allenfalls den EDÖB konsultieren (Art. 20 und 21 E-DSG).

- *Datenschutzberater:* Verantwortliche können einen Datenschutzberater ernennen und in der Folge von gewissen Erleichterungen profitieren (d.h. keine Konsultation des EDÖB bei Folgeabschätzung erforderlich) (Art. 9 E-DSG).
- *Privacy by Design:* Ein Unternehmen muss die Datenbearbeitung technisch und organisatorisch so ausgestalten, dass die Datenschutzvorschriften eingehalten werden (Art. 6 E-DSG).
- *Privacy by Default:* Ein Unternehmen muss für datenschutzrechtliche Voreinstellungen sorgen (Art. 6 E-DSG).
- *Datentransfer-Verträge:* Die Unterbeauftragung ist nur mit Genehmigung des Verantwortlichen zulässig (Art. 8 E-DSG).
- *Übermittlung ins Ausland mit Datenschutzklausel im Vertrag:* Personendaten dürfen ins Ausland bekannt gegeben werden, wenn geeignete Datenschutzklauseln vereinbart werden. Die Datenschutzklauseln gelten im Unterschied zu den Standarddatenschutzklauseln nur für die Bekanntgabe, die im entsprechenden Vertrag vorgesehen ist (Art. 13 E-DSG).
- *Übermittlung an ausländische Behörden:* Eine Übermittlung an ausländische Behörden ist zulässig, sofern dies zur Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen erforderlich ist (Art. 14 E-DSG). Dabei sind allerdings die Bearbeitungsgrundsätze einzuhalten.
- *Einverständliche Übermittlung ins Ausland:* Eine betroffene Person kann ausdrücklich einwilligen, dass ihre Daten in ein Land ohne angemessenen Datenschutz exportiert werden (Art. 14 E-DSG).
- *Keine Datenportabilität:* Das Prinzip der Datenportabilität wurde nicht ins E-DSG aufgenommen, weil die Thematik nicht das Datenschutzrecht, sondern das Konsumentenschutzrecht betrifft.
- *Begehren betroffener Personen:* Hinsichtlich der Begehren von betroffenen Personen (Auskunft, Berichtigung, Löschung, Widerspruch) bestehen verschiedene Neuerungen (Art. 23-25 und 28 E-DSG).
- *Datenspeicherung:* Personendaten müssen vernichtet oder anonymisiert werden, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind (Art. 5 E-DSG).

### Vergleich zwischen DSGVO und E-DSG

Das E-DSG enthält im Wesentlichen die neuen Regelungskonzepte, die in der DSGVO enthalten sind. Auf diese Weise soll die Schweiz im europäischen Kontext die Äquivalenz sicherstellen. Ihr Datenschutzniveau soll von der Europäischen Kommission als angemessen anerkannt werden, sodass Personendaten aus dem EU/EWR-Raum weiterhin ohne besondere Voraussetzungen in die Schweiz übermittelt werden können.

Es wäre wünschenswert, dass das E-DSG möglichst keine Anforderungen enthält, die über das Niveau der DSGVO hinausgehen (Swiss Finish). Die Befolgung der DSGVO sollte im Interesse der international tätigen Unternehmen grundsätzlich dazu führen, dass auch das DSG eingehalten wird.

## Umsetzung der neuen Pflichten

### Einwilligungserklärung

In der unternehmerischen Praxis wird der Einwilligung als Rechtfertigungsgrund eine grosse Bedeutung beigemessen. Bei genauer Betrachtung wird sie hingegen überbewertet. Erstens ist eine Einwilligung in vielen Fällen gar nicht nötig, wenn die Datenbearbeitung anderweitig gerechtfertigt werden kann. Zweitens ist die Einwilligung als Rechtfertigungsgrund nur beschränkt verfügbar, weil sie an verschiedene Voraussetzungen geknüpft ist, die im Einzelfall oftmals nicht erfüllt werden können. Drittens ist die Einwilligung nicht verlässlich, weil sie grundsätzlich widerrufen werden kann (vgl. Rosenthal, S. 15).

Die Anforderungen an eine gültige Einwilligung sind nach der DSGVO höher als nach dem E-DSG. Nach dem E-DSG muss nicht auf die Widerrufbarkeit der Einwilligung hingewiesen werden, besteht grundsätzlich kein Kopplungsverbot und sind vorangekreuzte Kästchen auf Online-Formularen an sich zulässig.

In der Praxis sollten Einwilligungserklärungen nur dort eingeholt werden, wo sie datenschutzrechtlich erforderlich sind. Einwilligungserklärungen müssen sorgfältig formuliert werden, um die gesetzlichen Gültigkeitsanforderungen zu erfüllen.

## Datenschutzerklärung

Verantwortliche müssen die betroffenen Personen über die Beschaffung von Personendaten informieren. Das gilt sowohl dann, wenn die Daten bei den betroffenen Personen erhoben werden, als auch dann, wenn die Daten anderweitig beschafft werden. Es besteht ein Katalog von Informationen, die mindestens enthalten sein müssen. In besonderen Fällen bestehen Einschränkungen und Ausnahmen. Die Informationen können mittels Standard-Informationsblättern (z.B. bei Versicherungsunternehmen nach Art. 3 VVG) und unter Umständen auch auf der eigenen Website zur Verfügung gestellt werden.

## Datenschutz-Folgeabschätzung

Es muss grundsätzlich eine Folgeabschätzung durchgeführt werden, wenn eine (geplante) Bearbeitung ein hohes Risiko für die Persönlichkeit der betroffenen Person mit sich bringen kann. Eine Folgeabschätzung enthält grundsätzlich folgende Elemente: (1) Beschreibung der geplanten Bearbeitung; (2) Beurteilung der Einhaltung der Datenschutzbestimmungen; (3) Identifikation und Dokumentation der möglichen Risiken der Datenbearbeitung; (4) Identifikation und Dokumentation der geplanten Massnahmen zum Schutz der betroffenen Personen. Die Datenschutzbehörde ist dann zu konsultieren, wenn die geplante Bearbeitung trotz der getroffenen Massnahmen immer noch ein hohes Risiko zur Folge hätte.

## Inventarpflicht

Der Verantwortliche und der Auftragsbearbeiter müssen ein Verzeichnis ihrer Bearbeitungstätigkeiten mit bestimmten Angaben erstellen. Dies kann für viele Betriebe eine Herausforderung darstellen. In der Schweiz kann der Bundesrat eine Ausnahme von dieser Pflicht vorsehen, wenn das Unternehmen weniger als 50 Mitarbeitende beschäftigt. Im EU/EWR-Raum greift unter bestimmten Voraussetzungen eine Ausnahme für Unternehmen ein, die weniger als 250 Mitarbeitende beschäftigen.

Für Auftragsbearbeiter dürfte die einfachste Methode zur Erfüllung der Inventarpflicht darin bestehen, eine Dokumentation der Verträge mit den Verantwortlichen zu führen. Diese Verträge enthalten für gewöhnlich die meisten Angaben, die erforderlich sind (vgl. Rosenthal, S. 23).

## Data Breach Notification

Der Verantwortliche muss der Aufsichtsbehörde eine Verletzung der Datensicherheit melden und diese unter Umständen den betroffenen Personen mitteilen. Ein Auftragsbearbeiter trifft eine Pflicht zur Meldung gegenüber dem Verantwortlichen. Eine Protokollierung der Verletzung der Datensicherheit ist nach der DSGVO, aber nicht nach dem E-DSG erforderlich.

Die Melde- und Mitteilungspflicht sollte im Rahmen eines unternehmensinternen Data-Breach-Prozesses spezifiziert werden. Es sollte spezifiziert werden, was ein melde- und mitteilungspflichtiger Data Breach ist. Es sollten die Zuständigkeiten und Abläufe (mit Fristen) festgelegt werden.

## Datenschutzberater / Datenschutzbeauftragter

Ein Datenschutzberater nach E-DSG hat lediglich eine beratende Funktion; es besteht anders als im Fall des betrieblichen Datenschutzbeauftragten nach DSGVO keine Ernennungspflicht für bestimmte Unternehmen. Den Datenschutzberater trifft in einer rein beratenden Rolle an sich kein datenschutzrechtliches Strafbarkeitsrisiko.

Der einzige Anreiz zur Ernennung eines Datenschutzberaters, der gegenwärtig im E-DSG vorgesehen ist, besteht darin, dass eine Datenschutz-Folgeabschätzung nicht mehr dem EDÖB vorgelegt werden muss. In der Lehre wird teilweise gefordert, dass weitere Erleichterungen vorgesehen werden, etwa eine Befreiung von der Data Breach Notification an den EDÖB.

## Vertragsanpassungen

Bei der Bekanntgabe von Personendaten ins Ausland sollte überprüft werden, ob die Verträge die erforderlichen Datenschutzklauseln bzw. die erforderlichen Standarddatenschutzklauseln enthalten. Die Verträge müssen soweit erforderlich angepasst werden.

## Dokumentationspflicht

Unternehmen sollten die Einhaltung der datenschutzrechtlichen Anforderungen angemessen dokumentieren. Eine solche Dokumentation kann bei einem späteren aufsichts-, straf- oder zivilrechtlichen Verfahren hilfreich sein. Anders als das E-DSG schreibt die DSGVO ausdrücklich vor, dass der Verantwortliche in der Lage sein muss, die Einhaltung der Bearbeitungsgrundsätze nachzuweisen.

### Interne Richtlinie

Die Unternehmen sollten eine Datenschutz-Richtlinie erlassen bzw. ihre Datenschutz-Richtlinie anpassen, um die Umsetzung der DSGVO und/oder des DSG zu regeln. Darin werden für gewöhnlich etwa neue Pflichten, Umsetzungsprozesse und Zuständigkeiten festgehalten.

## Verletzungsfolgen

### Verletzungsfolgen nach DSGVO

*Geldbussen und Strafen*

Im Rahmen der DSGVO können je nach Straftat folgende Geldbussen ausgesprochen werden: Geldbussen von bis zu 10‘000‘000 bzw. 20‘000‘000 Euro oder im Fall eines Unternehmens von bis zu 2% bzw. 4% seines gesamten weltweit erzielten Jahresumsatzes des vergangenen Geschäftsjahres, je nachdem, welcher der Beträge höher ist (Art. 83 Abs. 4 und 5 DSGVO). Neben den Geldbussen nach der DSGVO können die Mitgliedstaaten weitere strafrechtliche Sanktionen in ihren Umsetzungserlassen vorsehen. Beispielsweise sieht das deutsche BDSG Freiheits- und Geldstrafen für weitere strafrechtlich relevante Sachverhalte vor (§ 42 BDSG).

Das Verhängen von Geldbussen nach der DSGVO muss in jedem Einzelfall wirksam, verhältnismässig und abschreckend sein. Geldbussen können zusätzlich zu oder anstelle von verwaltungsrechtlichen Massnahmen verhängt werden. Bei der Entscheidung über die Verhängung einer Geldbusse und über den Bussbetrag müssen die verschiedenen Umstände des Einzelfalls berücksichtigt werden (Art. 83 Abs. 1 und 2 DSGVO).

*Administrative Durchsetzung*

Jede Aufsichtsbehörde hat erforderliche Untersuchungs- und Abhilfebefugnisse. Insbesondere kann sie einen Verantwortlichen oder einen Auftragsbearbeiter warnen, dass beabsichtigte Bearbeitungsvorgänge voraussichtlich gegen die DSGVO verstossen. Sie kann einen Verantwortlichen oder einen Auftragsbearbeiter verwarnen, wenn dieser mit Bearbeitungsvorgängen gegen die DSGVO verstossen hat. Sie kann einen Verantwortlichen oder einen Auftragsbearbeiter unter Strafandrohung anweisen, seinen Pflichten nach der DSGVO zu entsprechen, Personendaten zu berichtigen oder zu löschen oder eine Datenbearbeitung zu beenden (Art. 58 Abs. 1 und 2 DSGVO). Jeder Mitgliedstaat kann durch Rechtsvorschriften zusätzliche Befugnisse seiner Aufsichtsbehörde vorsehen (Art. 58 Abs. 6 DSGVO).

*Zivilrechtliche Durchsetzung und Schadenersatz*

Eine betroffene Person hat nach der DSGVO verschiedene Ansprüche gegenüber einem Unternehmen, das ihre Daten bearbeitet. Eine betroffene Person hat das Recht, eine abgegebene Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmässigkeit der aufgrund der Einwilligung bis zum Widerruf durchgeführten Bearbeitung nicht berührt (Art. 7 Abs. 3 DSGVO). Eine betroffene Person hat grundsätzlich das Recht, von dem Verantwortlichen Auskunft über die Bearbeitung sie betreffender Daten, die Berichtigung sie betreffender unrichtiger Daten, die Löschung sie betreffender Daten, die Einschränkung der Bearbeitung oder die Übertragung ihrer Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu verlangen (Art. 15 – 20 DSGVO). Wenn das Unternehmen einem berechtigten Begehren nicht entspricht, kann die betroffene Person das zuständige Zivilgericht im betreffenden EU/EWR-Mitgliedstaat anrufen und den Anspruch zivilrechtlich durchsetzen.

Jede Person, die wegen eines Verstosses gegen die DSGVO einen materiellen oder immateriellen Schaden erleidet, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsbearbeiter und kann beim zuständigen Zivilgericht des betreffenden EU/EWR-Mitgliedstaats Klage einreichen (Art. 82 Abs. 1 und 6 DSGVO). Jeder an einer Bearbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine verordnungswidrige Bearbeitung verursacht wurde. Ein Auftragsbearbeiter haftet für den durch eine Bearbeitung verursachten Schaden nur dann, wenn er seine speziell ihm auferlegten Pflichten verletzt oder Weisungen des Verantwortlichen missachtet hat (Art. 82 Abs. 2 DSGVO).

*Reputationsschaden:*

Wenn ein Verstoss gegen datenschutzrechtliche Vorschriften öffentlich bekannt wird, kann für das Unternehmen ein erheblicher Reputationsschaden resultieren. Das gilt auch im Fall der DSGVO. Unternehmen, die Personendaten bearbeiten, messen dem Reputationsschutz deshalb regelmässig erhebliche Bedeutung zu.

### Verletzungsfolgen nach E-DSG

*Geldbussen und Strafen*

Im Rahmen des E-DSG können Bussen bis zu CHF 250'000 ausgefällt werden (Art. 54-60 E-DSG). Im Rahmen des StGB sind Freiheitsstrafen und Geldstrafen vorgesehen.

*Administrative Durchsetzung*

Der EDÖB eröffnet von Amtes wegen oder auf Anzeige hin eine Untersuchung gegen ein Unternehmen, wenn Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte (Art. 43 E-DSG). Der EDÖB ist verpflichtet, Meldungen über mögliche Datenschutzverstösse nachzugehen. Zwar kann er von der Eröffnung einer Untersuchung absehen, wenn die Datenschutzverletzung von geringer Bedeutung ist. Doch macht der Entscheid darüber eine gewisse Auseinandersetzung mit der Sache erforderlich.

Kommt ein Unternehmen den Mitwirkungspflichten bei einer Untersuchung nicht nach, so kann der EDÖB den Zugang zu Räumlichkeiten oder die Herausgabe von Unterlagen anordnen (Art. 44 E-DSG). Liegt eine Verletzung von Datenschutzvorschriften vor, so kann der EDÖB verfügen, dass die Bearbeitung ganz oder teilweise angepasst, unterbrochen oder abgebrochen wird oder die Personendaten ganz oder teilweise gelöscht oder vernichtet werden (Art. 45 E-DSG).

*Zivilrechtliche Durchsetzung und Schadenersatz*

Eine betroffene Person hat nach dem E-DSG verschiedene Ansprüche gegenüber einem Unternehmen, das ihre Daten bearbeitet. Eine betroffene Person kann insbesondere verlangen, dass unrichtige Personendaten berichtigt werden, eine bestimmte Datenbearbeitung verboten wird, eine bestimmte Bekanntgabe von Personendaten an Dritte untersagt wird, Personendaten gelöscht oder vernichtet werden, ein Bestreitungsvermerk angebracht wird oder eine Veröffentlichung von Massnahmen erfolgt (Art. 28 E-DSG).

Jede Person, die wegen eines Verstosses gegen das DSG einen materiellen oder immateriellen Schaden erleidet, hat Anspruch auf Schadenersatz oder Genugtuung (Art. 28a Abs. 3 ZGB).

*Reputationsschaden:*

Wenn ein Verstoss gegen datenschutzrechtliche Vorschriften öffentlich bekannt wird, kann für das Unternehmen ein erheblicher Reputationsschaden resultieren. Das gilt auch im Fall des DSG.

### Vergleich zwischen DSGVO und E-DSG

Die angedrohten Bussen nach DSGVO sind bedeutend höher als jene nach E-DSG. Es wird sich die Frage stellen, ob dieser Unterschied bei der datenschutzrechtlichen Durchsetzung einer Anerkennung des E-DSG als angemessene Regelung durch die Europäische Kommission entgegensteht.

Während sich die strafrechtliche Sanktionierung nach DSGVO gegen das Unternehmen richtet (finanzielle Verwaltungssanktionen), richtet sich die Strafandrohung nach E-DSG vor allem gegen die zuständigen natürlichen Personen.

Anders als die Aufsichtsbehörden im EU/EWR-Raum hat der EDÖB keine Strafkompetenz. Die Verfolgung und Beurteilung strafbarer Handlungen obliegt den Kantonen. Der EDÖB kann immerhin bei der zuständigen Strafverfolgungsbehörde Anzeige erstatten (Art. 59 E-DSG).

## Räumlicher Geltungsbereich

### Geltungsbereich der DSGVO

*Niederlassung im EU/EWR-Raum*

Schweizer Unternehmen unterstehen räumlich der DSGVO, soweit sie im EU/EWR-Raum eine Niederlassung haben. Art. 3 Abs. 1 DSGVO enthält folgende Regelung zum räumlichen Geltungsbereich: „*Diese Verordnung findet Anwendung auf die Bearbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsbearbeiters in der Union erfolgt, unabhängig davon, ob die Bearbeitung in der Union stattfindet.*"

Es ergibt sich, dass jede Bearbeitung von Personendaten durch ein Schweizer Unternehmen im Rahmen der Tätigkeiten einer Niederlassung im EU/EWR-Raum der DSGVO untersteht, gleichgültig, ob die Bearbeitung in oder ausserhalb des EU/EWR-Raums stattfindet. Es kommt allein darauf an, ob im Rahmen der Geschäftstätigkeit der EU/EWR-Niederlassung Personendaten bearbeitet werden.

Dabei setzt eine Niederlassung die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus. Auf die Rechtsform kommt es dabei nicht an. Es kann sich um eine Zweigniederlassung oder eine Tochtergesellschaft mit eigener Rechtspersönlichkeit handeln (Einleitungsziffer 22 DSGVO).

### *Keine Niederlassung im EU/EWR-Raum*

Schweizer Unternehmen können räumlich der DSGVO selbst dann unterstehen, wenn sie keine Niederlassung im EU/EWR-Raum haben. Art. 3 Abs. 2 DSGVO enthält folgende Regelung zum räumlichen Geltungsbereich („*Marktortprinzip*"): „*Diese Verordnung findet Anwendung auf die Bearbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsbearbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht (a) betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist; (b) das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.*"

Es ergibt sich, dass für die Anwendung der DSGVO keine Niederlassung im EU/EWR-Raum erforderlich ist, wenn die Datenbearbeitung dazu dient, betroffenen natürlichen Personen, die sich im EU/EWR-Raum befinden, Waren oder Dienstleistungen anzubieten. Dabei kommt es darauf an, ob offensichtlich beabsichtigt ist, betroffenen Personen in einem oder mehreren EU/EWR-Mitgliedstaaten Waren oder Dienstleistungen anzubieten. Unternehmen mit Sitz ausserhalb des EU/EWR-Raums haben dieselben Regeln anzuwenden wie Unternehmen mit Sitz im EU/EWR-Raum. Auf diese Weise wird der Schutz der Rechte von Bürgern im EU/EWR-Raum sichergestellt und es werden gleiche Wettbewerbsbedingungen für Unternehmen im EU/EWR-Raum und Unternehmen ausserhalb des EU/EWR-Raums geschaffen (Zerdick, Art. 3 Rz 2).

Es ergibt sich weiter, dass die DSGVO auch ohne Niederlassung im EU/EWR-Raum zur Anwendung kommt, wenn die Bearbeitung der Daten von betroffenen natürlichen Personen, die sich im EU/EWR-Raum befinden, dazu dient, das Verhalten dieser betroffenen Personen zu beobachten, soweit ihr Verhalten im EU/EWR-Raum erfolgt. Ob eine relevante Verhaltensbeobachtung vorliegt, sollte daran festgemacht werden, ob ihre Internetaktivitäten nachvollzogen werden, inklusive der möglichen nachfolgenden Verwendung von Techniken zur Bearbeitung von Personendaten, durch die von einer natürlichen Person ein Profil erstellt wird, das insbesondere die Grundlage für sie betreffende Entscheidungen bildet oder anhand dessen ihre persönlichen Vorlieben, Verhaltensweisen oder Gepflogenheiten analysiert oder prognostiziert werden sollen (Einleitungsziffer 24 DSGVO). Es fallen insbesondere jegliche Formen des Trackings (Beobachten, Sammeln, Auswerten des Surfverhaltens betroffener Personen im Internet) und das Profiling (Erstellen von Profilen von Kunden, Mitarbeitenden oder anderen, um bestimmte persönliche Aspekte wie Leistung, Gesundheit, Aufenthaltsorte etc. zu bewerten oder Vorhersagen zu treffen) im Internet durch Analyse-Tools, die wie beispielsweise Cookies die individuelle Rückverfolgbarkeit der Nutzer ermöglichen oder zum Zweck der individuellen Werbung (targeted advertising) erfolgen, unter die Bestimmung (Kurzpapier 7 der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz –DSK), Marktortprinzip: Regelungen für aussereuropäische Unternehmen, Stand: 26. Juli 2017; vgl. zu „Profiling" auch Rosenthal, S. 9 ff.).

### *Grenzüberschreitende Auftragsbearbeitung*

Wenn ein Schweizer Unternehmen als Verantwortlicher seine Daten von einem Auftragsbearbeiter im EU/EWR-Raum bearbeiten lässt (z.B. Cloud), ist die DSGVO direkt auf den Auftragsbearbeiter anwendbar. Es ist hingegen nicht klar, wie es sich mit dem verantwortlichen Schweizer Unternehmen verhält. Wenn es nicht der DSGVO unterliegt, muss es vertraglich in die Pflicht genommen werden. Die Rechtslage ist unklar.

Wenn ein Schweizer Unternehmen als Auftragsbearbeiter für ein Unternehmen im EU/EWR-Raum Dienstleistungen erbringt, ist die DSGVO direkt auf das verantwortliche Unternehmen anwendbar. Es ist aber nicht klar, wie es sich mit dem Schweizer Dienstleister verhält. Wenn er nicht der DSGVO unterstellt ist, muss er vertraglich verpflichtet werden. Die Rechtslage bedarf einer weiteren Klärung.

### *Anwendung der DSGVO vermeiden*

Schweizer Unternehmen können die Anwendung der DSGVO allgemein dadurch vermeiden, dass sie keine Personendaten im EU/EWR-Raum (grenzüberschreitend oder über eine Niederlassung) zum Zweck der eigenen Geschäftstätigkeit erheben und bearbeiten.

Schweizer Unternehmen, die die Anwendung der DSGVO vermeiden wollen, sollten insbesondere sicherstellen, dass sich aus dem eigenen Internetauftritt keine Absicht erkennen lässt, betroffenen Personen in einem oder mehreren EU/EWR-Mitglied-staaten Waren oder Dienstleistungen anzubieten. Die blosse Zugänglichkeit der Website des Verantwortlichen, des Auftragsbearbeiters oder eines Vermittlers im EU/EWR-Raum, einer E-Mail-Adresse oder anderer Kontaktdaten oder die Verwendung einer Sprache, die in dem Drittland, in dem der Verantwortliche niedergelassen ist, sind allgemein gebräuchlich und hierfür kein ausreichender Anhaltspunkt. Hingegen können andere Faktoren darauf hindeuten, dass der Verantwortliche beabsichtigt, den Personen im EU/EWR-Raum Waren oder Dienstleistungen anzubieten, wie etwa die Verwendung einer Sprache oder Währung, die in einem oder mehreren Mitgliedstaaten gebräuchlich ist, in Verbindung mit der Möglichkeit, Waren und Dienstleistungen in dieser anderen Sprache zu bestellen, oder die Erwähnung von Kunden oder Nutzern, die sich im EU/EWR-Raum befinden (Einleitungsziffer 23 DSGVO).

Der rein zu Präsentationszwecken erfolgte Webauftritt eines Schweizer Unternehmens stellt keine relevante Dienstleistung in diesem Sinne dar. Es ist auch nicht ausreichend, mittels einer Website die Dienste lediglich zugänglich zu machen (Pilz, Art. 3 Rz 28). Hingegen ist gegenwärtig noch unklar, ab wann die Beobachtung des Verhaltens von europäischen Besuchern der Webseite ein Tracking oder Profiling darstellt. Deshalb wird Schweizer Unternehmen, die eine Anwendung der DSGVO vermeiden wollen, zurzeit teilweise empfohlen, europäische Besucher im Sinne eines „dis-targetings“ vom Tracking oder Profiling auszunehmen (vgl. Peter, S. 1 ff; Klar, Art. 3 Rz 101).

### Geltungsbereich des E-DSG

Der räumliche Geltungsbereich des E-DSG ist breit und richtet sich im internationalen Verhältnis nach dem IPRG. Art. 139 Abs. 3 IPRG bestimmt, dass das anwendbare Recht im Fall einer Persönlichkeitsverletzung auch anwendbar ist auf Ansprüche aus Verletzung der Persönlichkeit durch das Bearbeiten von Personendaten sowie aus Beeinträchtigung des Rechts auf Auskunft über Personendaten. Dementsprechend kommt das DSG je nach Wahl des Geschädigten zur Anwendung, wenn der Geschädigte seinen gewöhnlichen Aufenthalt in der Schweiz hat, wenn der Verantwortliche oder der Auftragsbearbeiter seine Niederlassung in der Schweiz hat oder wenn der Erfolg der verletzenden Handlung in der Schweiz eintritt (Art. 139 Abs. 1 IPRG).

Es ergibt sich, dass Unternehmen in der Schweiz, die Personendaten bearbeiten, und Unternehmen ausserhalb der Schweiz, die Daten von betroffenen Personen in der Schweiz bearbeiten, grundsätzlich unter den Geltungsbereich des DSG fallen.

### Vergleich zwischen DSGVO und E-DSG

Sowohl die DSGVO als auch das E-DSG kennen einen extensiven räumlichen Geltungsbereich zum Schutz der betroffenen Personen. Die DSGVO kann auf Datenbearbeitungen und Datenbearbeiter in der Schweiz zur Anwendung kommen. Umgekehrt kann das E-DSG auf Datenbearbeitungen und Datenbearbeiter ausserhalb der Schweiz zur Anwendung kommen.

Es ergibt sich, dass Schweizer Unternehmen gleichzeitig unter den Geltungsbereich der DSGVO und den Geltungsbereich des E-DSG fallen können. Sie müssen dann sowohl die Anforderungen nach der DSGVO als auch jene nach dem E-DSG erfüllen. In solchen Fällen können sich Schweizer Unternehmen entschliessen, für alle Datenbearbeitungen die Anforderungen nach der DSGVO umzusetzen. Da diese Anforderungen im Regelfall über jene des E-DSG hinausgehen, werden für gewöhnlich auch die Anforderungen nach dem E-DSG erfüllt. Alternativ können sich Schweizer Unternehmen entschliessen, die verschiedenen Datenbearbeitungen zuzuordnen und dabei von Fall zu Fall die DSGVO oder das DSG umzusetzen. Letzteres macht vor allem Sinn, wenn ein Schweizer Unternehmen nur in marginalen Bereichen (z.B. Tracking von Benutzern auf eigener Website) der DSGVO unterstellt ist.

## Literaturverzeichnis


Klar Manuel, in: Jürgen Kühling und Benedikt Buchner (Hrsg.), Datenschutz-Grundverordnung, Kommentar C.H. Beck, 2017

Peter Christian, DSGVO und E-DSG fordern Schweizer Spitäler, Heime und Spitex, in Jusletter 26. Februar 2018

Pilz Carlo, in: Peter Gola (Hrsg.), Datenschutz-Grundverordnung, C.H. Beck 2017

Rosenthal David, Der Entwurf für ein neues Datenschutzgesetz, in: Jusletter 27. November 2017

Unabhängige Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz –DSK), Kurzpapier 7,

Marktortprinzip: Regelungen für aussereuropäische Unternehmen, Stand: 26. Juli 2017

Zerdick Thomas, in: Eugen Ehmann und Martin Selmayr (Hrsg.), DS-GVO, Datenschutz-Grundverordnung, Kommentar, 2017

## Abkürzungsverzeichnis

| | |
|---|---|
| AGB | Allgemeine Geschäftsbedingungen |
| BDSG | Deutsches Bundesdatenschutzgesetz, revidiert im Jahr 2017 |
| DSGVO | Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Bearbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DS-Grundverordnung) |
| E-DSG | Entwurf des revidierten Datenschutzgesetzes der Schweiz |
| EDÖB | Eidg. Datenschutz- und Öffentlichkeitsbeauftragter |
| EU | Europäische Union |
| EWR | Europäischer Wirtschaftsraum |
| IPRG | Bundesgesetz über das internationale Privatrecht von 1987 |
| StGB | Schweizerisches Strafgesetzbuch |

## Weitere Publikationen im Datenschutzrecht

- Risikobasierte Umsetzung der DSGVO durch Schweizer Unternehmen, 2018 (d)
- Regelung des Datenschutzes im multinationalen Konzern (eine Übersicht), 2014 (d/e)
- Entwicklungen im Unternehmens-Datenschutzrecht der Schweiz und der EU, 2012 (d)
- Entwicklungen im Unternehmens-Datenschutzrecht der Schweiz und der EU, 2010
- Entwicklungen im Datenschutzrecht für Unternehmen in der Schweiz und der EU, 2009-2 (d)
- Entwicklungen im Datenschutzrecht für Unternehmen in der Schweiz und der EU, 2009-1 (d/e)
- Revidiertes Datenschutzrecht für Unternehmen in der Schweiz, 2007 (d)
- Dokumenten- und Datenaufbewahrung im schweizerischen Unternehmen, 2006 (d)