# Welche Regelungen beinhaltet die Europäische Datenschutz-Grundverordnung - DSGVO-EU?

# Persönliche Daten dürfen nur genutzt werden, wenn eine frei abgegebene, spezifische und informierte Einwilligung des Betroffenen vorliegt. Schweigen oder Inaktivität dürfen nicht als Einwilligung interpretiert werden.

Eine Datenverarbeitung darf darüber hinaus auch beim Nachweis der Notwendigkeit für das Verfolgen "legitimer Interessen" erfolgen, allerdings nur unter der Voraussetzung, dass dadurch nicht die Grundrechte des "Datensubjekts" unterwandert werden.

Für das Erstellen von Nutzerprofilen gelten ähnliche Anforderungen, Ausnahmen gibt es für statistische und Forschungszwecke und beim Verwenden pseudonymisierter oder anonymer Daten.

## Europäisches Datenschutz Gütesiegel

Die Datenschutz-Grundverordnung schlägt zudem die Vergabe eines "Europäischen Datenschutz-Gütesiegels" vor, um das Vertrauen von Nutzern in entsprechend zertifizierte Dienste sowie die Rechtssicherheit für Anbieter zu erhöhen. Daneben gibt es eine Klausel, wonach Telekommunikations- und Internetkonzerne Daten nur auf Grundlage europäischen Rechts oder vergleichbarer Abkommen an Behörden in Drittstaaten wie die USA übermitteln dürften.

## Informationsrechte

Die DSGVO gibt Betroffenen weitreichende Informationsrechte ein. Beispielsweise ist eine Informationspflicht über die Dauer der Datenspeicherung vorgesehen.

## Betrieblicher Datenschutzbeauftragter

Ein betrieblicher Datenschutzbeauftragter muss grundsätzlich bestellt werden, wenn die verantwortliche Stelle in 12 Monaten die Daten von mehr als 5.000 Betroffenen verarbeitet. Noch weitergehend müssen auch verantwortliche Stellen, die besonders sensible Datenverarbeitungen betreiben, einen Datenschutzbeauftragten bestellen.

## Sanktionen

Die geplante Europäische Datenschutz-Grundverordnung sieht als Höchststrafe für Verstöße 100 Millionen Euro oder fünf Prozent des Jahresumsatzes eines Unternehmens vor, je nachdem, welcher

Wert der höhere ist. Das dadurch entstehende finanzielle Risiko ist mit demjenigen bei Kartellrechtsverstößen somit durchaus vergleichbar.

Unternehmen müssen somit in wichtigen Datenverarbeitungsbereichen regelmäßige Compliance-Audits durchzuführen, um das Risiko kostenträchtiger Datenschutzverstöße zu minimieren. Sie müssen eine Risikoanalyse und eine Folgenabschätzung durchführen und die Einhaltung der Regeln alle zwei Jahre durch einen externen Experten überprüfen lassen.

### Verbandsklage

Die EU-DSGVO sieht in den Art. 73 ff. ein Verbandsklagerecht vor. Die Daten verarbeitenden Unternehmen sind dann gerichtlichen Auseinandersetzungen über Datenschutzverstöße ausgesetzt. Der Verband kann in Vertretung zumindest einer betroffenen Person aber nicht nur vor Gericht, sondern auch bei den Datenschutzaufsichtsbehörden ein Verfahren wegen der Verletzung von Datenschutzvorschriften einleiten. Betroffene haben zudem das Recht, auch immateriellen Schadensersatz zu verlangen. Bei Verstößen gegen das Datenschutzrecht treffen die Unternehmen somit neben sehr hohen Geldbußen auch nicht unerhebliche private Schadensersatzforderungen.

### Haftung des Auftragsdatenverarbeiters gegenüber den Betroffenen

Gem. Art 77 DSGVO wird der Anspruch auf Ersatz des Schadens, der dem Betroffenen durch die unrechtmäßige Verarbeitung seiner Daten entstanden ist, und der sich gegen die datenverantwortliche Stelle richtet, auf Auftragsdatenverarbeiter ausgeweitet. Der Betroffene kann somit seinen Schaden gegenüber mehreren Stellen einklagen, die als Gesamtschuldner haften. Sowohl die verantwortliche Stelle als auch der Auftragsdatenverarbeiter können die Haftung abwenden, wenn sie nachweisen, dass sie das den Schaden auslösende Ereignis nicht verschuldet haben. Wenn mehrere Daten verarbeitende Stellen beteiligt sind, haftet jede Stelle gegenüber dem Betroffenen in Höhe des vollen Schadens.

Betroffene können auch den Ersatz immaterieller Schäden verlangen.

## Allgemeine Informationspflicht bei Datenpannen

Im Fall eines Datenverlustes müssen die Betroffenen und gleichzeitig die zuständige Datenschutzaufsichtsbehörde informiert werden. Datenschutzpannen sind "ohne ungerechtfertigte Verzögerung", also i.d.R. binnen 72 Stunden den Betroffenen mitzuteilen.

## Anforderungen an die Datenschutz-Compliance

### Compliance-Nachweise

Entsprechend Art. 22 Nr. 1 der DSGVO müssen datenverantwortliche Stellen Datenschutz-Policies und geeignete technische und organisatorische Maßnahmen vorhalten, um die Einhaltung der DSGVO nachzuweisen. Zudem besteht die Verpflichtung, diese alle 2 Jahre zu überarbeiten.

Gemäß Art. 23 DSGVO muss die datenverantwortliche Stelle (und ggf. auch der Auftragsdatenverarbeiter) darauf achten, dass sowohl die Systeme, mit denen personenbezogene Daten verarbeitet werden, als auch die entsprechenden Arbeitsabläufe datenschutzfreundlich gestaltet sind.

### Durchführung von Folgenabschätzungen

Gem. Art. 32a ff. DSGVO sind die datenverantwortliche Stelle als auch der Auftragsdatenverarbeiter verpflichtet, im Vorfeld der geplanten Datenverarbeitung Risikoanalysen und datenschutzrechtliche Folgenabschätzungen durchzuführen. Für den Fall, dass dann besondere Risiken festgestellt werden, muss u.U. die zuständige Datenschutzaufsichtsbehörde unterrichtet werden, die die geplante Datenverarbeitung ggf. sogar untersagen kann. Die Risikoanalysen und Folgenabschätzungen müssen laufend in der Form eines kontinuierlichen Datenschutz Lifecycle-Management überprüft und untersucht werden.

## Erweiterte Transparenzpflichten durch Datenschutzerklärungen

Die Art. 11 ff. DSGVO erweitern die Transparenzanforderungen. Die für die Datenverarbeitung verantwortlichen Stellen sind angehalten, Datenschutzerklärungen über die von ihnen vorgenommene Datenverarbeitung zu erstellen. Sie müssen darin aufführen, wie die betroffenen Personen ihre Rechte, z. B. auf Auskunft oder Löschung, ausüben können. Diese Datenschutzerklärung muss allgemein verständlich und einfach zugänglich sein.

Art. 12 DSGVO sieht vor, dass die datenverantwortliche Stelle auch darüber informieren muss, wie lange die verarbeiteten Daten gespeichert werden.

Gem. Art. 13a DSGVO muss die verantwortliche Stelle die Betroffenen durch eine standardisierte Tabelle darüber informieren, wie sie mit personenbezogenen Daten verfährt. Durch an Verkehrsschilder angelehnte Abbildungen ist der Betroffene etwa darüber in Kenntnis zu setzen, ob personenbezogene Daten an Dritte übermittelt werden oder in unverschlüsselter Form aufbewahrt werden.

## Einrichtung eines Verfahrens zur Ausübung der Betroffenenrechte

Gemäß Art. 12 DSGVO müssen die datenverantwortlichen Stellen elektronische Verfahren einrichten, mittels derer die von der Datenverarbeitung betroffenen Personen ihre Betroffenenrechte, wie z. B. auf Auskunft oder Löschung, geltend machen können.

Auf eine Anfrage der Betroffenen muss die verantwortliche Stelle innerhalb von 40 Kalendertagen antworten. In Ausnahmefällen darf die Antwort einen Monat später erfolgen.

## Recht auf Löschung und Berichtigung

Art. 17 der DSGVO sieht ein Recht auf Berichtigung und Löschung vor. Mit diesem Recht korrespondieren Löschungsverpflichtungen der verantwortlichen Stelle.

Soweit sie Daten des Betroffenen öffentlich gemacht hat, ist gemäß Art. 17 Nr. 2 DSGVO die verantwortliche Stelle verpflichtet, alle vernünftigen Maßnahmen zu ergreifen, um diese Daten auch bei Dritten löschen zu lassen.

## Datenportabilität

Auf Anfrage müssen die datenverantwortlichen Stellen den betroffenen Personen die von ihnen verarbeiteten Daten elektronisch zur Verfügung stellen, wenn sie deren Daten automatisiert verarbeiten. Das soll den betroffenen Personen vor allem ermöglichen, Daten aus sozialen Netzwerken zu einem anderen Anbieter zu portieren.

## Konzernprivileg

Art. 22 Abs. 3a DSGVO konstituiert eine Art Konzernprivileg. Danach können gruppeninterne Datenweitergaben zwischen verbundenen Unternehmen unter erleichterten Voraussetzungen erfolgen. Voraussetzung ist allerdings, dass ein angemessenes Datenschutzniveau gewährleistet ist. Dass kann etwa durch gruppeninterne vertragliche Regelungen oder branchenweite Codes of Conduct geschehen.

## Angemessenheit des Datenschutzniveaus in Drittländern

Art. 41 der DSGVO sieht vor, dass die EU-Kommission nunmehr auch die Angemessenheit des Schutzniveaus für einzelne Territorien und bestimmte Verarbeitungssektoren innerhalb eines Drittstaates feststellen kann, in die Daten anschließend übermittelt werden dürfen.

So können etwa auch einzelne Bundesstaaten in einem Drittland anerkannt werden.

## Binding Corporate Rules

Art. 43 DSGVO sieht vor, dass auch Binding Corporate Rules einen Datentransfer in Drittländer rechtfertigen können. Derartige Binding Corporate Rules müssen zuvor anerkannt werden. Die Genehmigung zum Datentransfer muss (nur) von einer einzigen Datenschutzaufsichtsbehörde erteilt werden.

## Auskunft an Behörden oder Gerichte aus Drittstaaten

Art. 43a DSGVO regelt die Übermittlung von Daten an Behörden oder Gerichte in Drittstaaten. Im Fall von Anfragen dieser Stellen, etwa aufgrund von Urteilen oder bindenden Entscheidungen, sollen die Daten verarbeitenden Stellen die Datenschutzaufsichtsbehörden benachrichtigen. Diese klären anschließend, ob und inwiefern Daten übermittelt werden dürfen.

## Zusammenarbeit der Datenschutzbehörden

Die DSGVO gibt die Regeln vor, wie die Datenschutzaufsichtsbehörden innerhalb der EU zusammenarbeiten. Es wird ein neues Gremium, das "European Data Protection Board", geschaffen, das aus den jeweiligen Leitern aller nationalen Datenschutzbehörden in Europa besteht. Für den Fall, dass in einem Land (Beispiel: Deutschland) mehrere Datenschutzbehörden bestehen, sollen die nationalen Datenschutzbehörden das Mitglied bestimmen. Das European Data Protection Board koordiniert die nationalen Datenschutzbehörden und hat Entscheidungsbefugnisse im Fall von Streitigkeiten zwischen zwei Datenschutzaufsichtsbehörden aus verschiedenen EU-Mitgliedstaaten.

Maßnahmen einer Datenschutzbehörde können auch in einem anderen von dem Fall betroffenen EU-Mitgliedstaat durchgesetzt werden.

Für einen Fall ist zukünftig nur noch eine Datenschutzaufsichtsbehörde zuständig, selbst dann, wenn eine Untersuchung eine Datenverarbeitung in mehreren EU-Mitgliedstaaten betrifft. Zuständig ist die Datenschutzaufsichtsbehörde in dem EU-Mitgliedstaat, in dem die verantwortliche Stelle ihren Hauptsitz hat.

## Personenbezug von IP-Adressen

Aus Art. 4 Nr. 1 der DSGVO i. V. m. Erwägungsgrund folgt, dass IP-Adressen nicht generell als personenbezogene Daten eingestuft werden.

Das ist jedoch sehr umstritten.

## Schutz von Kindern

Die Daten von Kindern unter 13 Jahren dürfen nur noch aufgrund einer Einwilligung der Erziehungsberechtigten verarbeitet werden. Damit wird der datenrechtliche Schutz von Kindern erweitert.

**Quelle:** [**http://www.europaeische-datenschutz-grundverordnung.de**](http://www.europaeische-datenschutz-grundverordnung.de)