

# Die EU-DSGVO kommt

## Auswirkungen der EU-Datenschutzgrundverordnung für private Anwender und Unternehmen

Evren Eren, Eda Tasdelen

Am 25. Mai 2018 muss die EU-Datenschutzgrundverordnung (EU-DSGVO) eingeführt sein und wird damit direkt geltendes Recht in allen Mitgliedstaaten. Zuvor verabschiedete die Bundesregierung bereits den Gesetzentwurf für das neue, an die EU-DSGVO angepasste Bundesdatenschutzgesetz (BDSG). In beiden, sowohl in der EU-DSGVO als auch im BDSG, stehen sowohl der Schutz personenbezogener Daten als auch der freie Datenverkehr innerhalb des europäischen Marktes im Vordergrund.



Für interessierte NET-Abonnenten steht das Literaturverzeichnis zu diesem Beitrag im Heftarchiv 3/18 unter [www.NET-im-web.de](http://www.NET-im-web.de).

Prof. Dr. Evren Eren ist Professor am Lehrstuhl für IT-Sicherheitsarchitekturen an der Hochschule Bremen, Eda Tasdelen ist Masterstudentin an der Hochschule Bremen

Das im Jahr 1977 verfasste BDSG regelt die Datenschutzgesetze in der Bundesrepublik Deutschland. Dabei stehen personenbezogene Daten und Persönlichkeitsrechte im Vordergrund. Es beschreibt „technische und organisatorische Maßnahmen“, um die unerlaubte Verarbeitung von Daten verhindern zu können. Dabei werden sowohl im Internet als auch in Unternehmen und abseits der elektronischen Vernetzung anfallende Daten berücksichtigt [1], [2].

### EU-Datenschutzgrundverordnung

Die EU-Datenschutzgrundverordnung ist die „Modernisierung und Anpassung der bestehenden Datenschutzregeln“ in den europäischen Mitgliedstaaten mit dem Ziel, ein gleichwertiges Datenschutzniveau innerhalb der EU abzubilden [3]. Sie tritt am 25. Mai 2018 in Kraft. Die Verordnung benötigt kein Gesetzgebungsverfahren im Bundestag, da sie auf nationaler Rechtsordnung wirkt. Sie ist nicht in jedem Detail bestimmt, sondern besitzt einige „Öffnungsklauseln“, die von einzelnen Mitgliedstaaten genauer definiert werden können, wie z.B. Sachverhalte, Rechte und Pflichten [4].

### BDSG-Neu

Das neue BDSG wurde an die europäischen Vorgaben der EU-DSGVO angepasst und ersetzt somit das vierzig



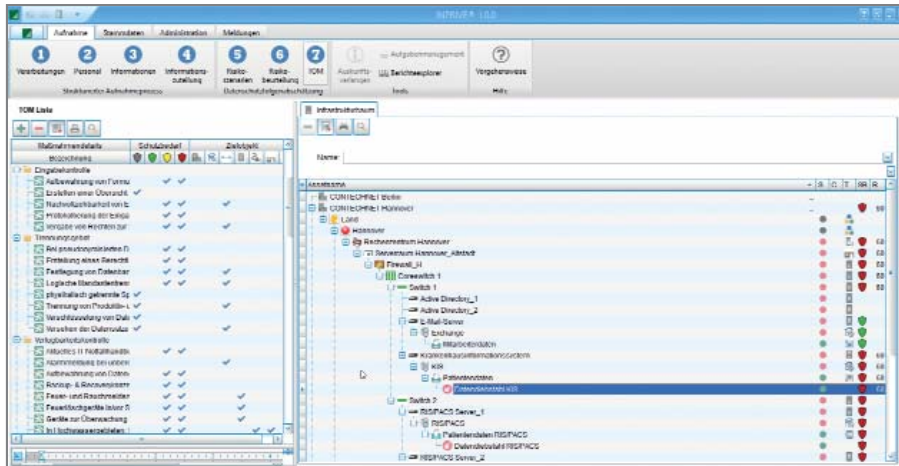
Der Weg der Daten lässt sich in fünf Phasen gliedern: Collect (Sammeln), Transport (Transportieren), Store (Speichern), Analyze (Analysieren) und Archive (Archivieren) (Quelle: Netapp)

Jahre alte BDSG. Das jetzige BDSG wird vollständig aufgehoben.

Die EU-DSGVO enthält Vorschriften, die zum Schutz von personenbezogenen Daten dienen und die Weitergabe an Dritte regeln. Dabei schützt die Verordnung die Grundrechte und Grundfreiheiten von Personen und ihrer Daten [5]. Die Datenverarbeitung steht im neuen BDSG im Vordergrund, wird aber auch in der EU-DSGVO zum Großteil geregelt.

Die Öffnungsklauseln der EU-DSGVO dienen zur spezifischen und konkreten Ausarbeitung von Regelungen, die in den Mitgliedstaaten eindeutig definiert und erweitert werden können. Dabei schreibt der Erwägungsgrad Acht der EU-DSGVO vor, dass im Fall von gewünschten Präzisierungen oder Einschränkungen in den Mitgliedstaaten die Verordnung in das nationale Recht aufgenommen werden darf, um „nationale Rechtsvorschriften für die Personen, für die sie gelten, verständlicher zu machen.“

Da das BDSG-Neu auf viele Paragraphen der EU-DSGVO verweist, ist das neue Datenschutzgesetz in Deutsch-



Die Datenschutzsoftware Inprive leitet den Anwender Schritt für Schritt durch die Umsetzung der EU-DSGVO-Anforderungen (Quelle: Contechnet)

land sehr komplex und für viele Datenschutzexperten schwer verständlich [6].

Im BDSG-Neu sollen die Informationsrechte betroffener Personen nicht mehr grundsätzlich, sondern nur bei Zweckänderung beschränkt werden. Außerdem ist der Beschäftigtendatenschutz detaillierter geregelt als im vorherigen § 32 des BDSG.

Grundsätzlich lässt sich sagen, dass in Deutschland im Vergleich zu anderen Ländern nicht viel geändert wird, da die EU einige Anforderungen des BDSG in die EU-DSGVO übernommen hat. Dennoch bestehen Unterschiede zwischen dem BDSG-Neu und der EU-DSGVO.

Eine Abweichung ist z.B. die Regelung zum Datenschutzbeauftragten. Die BDSG-Neu übernimmt die bisherigen Regeln des alten BDSG und stärkt somit die Stellung des Datenschutzbeauftragten, da die EU-DSGVO nicht auf die Befugnisse und Rechte des Datenschutzbeauftragten im Sinne der BRD eingeht. So erhält der Datenschutzbeauftragte zum Beispiel einen umfassenden Kündigungsschutz, den die EU-DSGVO nicht vorschreibt [3].

### Auswirkungen auf Unternehmen

Die EU-DSGVO ist seit 2016 in Kraft und muss bis zum 25. Mai 2018 in Unternehmen vollständig eingeführt werden. Dabei müssen sie viele Änderungen berücksichtigen:

- Bis zum Inkrafttreten sollten Verträ-

ge und Prozesse auf das neue Gesetz angepasst werden.

- Bei Datenschutzverstößen müssen Unternehmen Geldstrafen in Höhe von 20 Mio. € oder 4 % des weltweiten Jahresumsatzes befürchten (Art. 83 DSGVO, Absatz 5) [7], [8].
- Erhält ein Unternehmen durch einen Kaufvertrag personenbezogene Daten, ist er nicht automatisch dafür autorisiert, diese für andere Zwecke zu nutzen oder zu ändern.
- Außerdem besitzen Privatpersonen Anspruch auf das Löschen ihrer Daten. Somit müssen Unternehmen die gesammelten Daten, die sie veröffentlicht haben, löschen und die Aufforderung zum Löschen der Daten des Nutzers auch an andere Konzerne mitteilen, die mit diesen Daten gearbeitet haben [9].
- US-Unternehmen, die in europäischen Ländern Dienste anbieten, müssen die EU-DSGVO und die Gesetze des jeweiligen EU-Mitgliedstaates beachten. Unternehmen aus Drittstaaten (Google, Facebook, Microsoft ...) müssen demnach „einen Vertreter für die EU benennen, der als Anlaufstelle und Ansprechpartner für Betroffene und Aufsichtsbehörden fungiert.“ Dies könnte letztendlich Auswirkungen auf europäische Bürger haben, da amerikanische Konzerne ihre Dienste verweigern können, so dass für EU-Bürger diese dann nicht mehr nutzbar sind. Vor der Einführung der EU-DSGVO galt das Sitzlandprinzip, das besagt, dass bei „juristischen Konflikten die Gesetze des Landes [...]“ in Kraft

treten, „in dem das Unternehmen seinen Hauptsitz hat“ [9].

- Unternehmen müssen durch Nachweise und Zertifikate die Datenverarbeitung belegen können. Falls Daten fehlerhaft oder falsch verarbeitet werden, müssen sie sich an die Privatperson wenden, von der die Daten stammen. Unternehmen sollten daher
  - verhindern, dass der falsche Vorgang eintritt, damit sie nicht Bußgelder zahlen müssen;
  - verstehen, wie der falsche Vorgang eintrat, damit Fehler sich nicht wiederholen;
  - den falschen Vorgang so schnell wie möglich korrigieren;
  - nachweisen, dass der falsche Vorgang korrigiert wurde [10].

### Auswirkungen im privaten Bereich

Auch der private Bereich ist betroffen. Privatpersonen können vom neuen Recht profitieren.

- Laut Artikel 7 und 8 der EU-DSGVO benötigen Unternehmen zur Datenverarbeitung explizit das persönliche Einverständnis des Nutzers, mit dem Recht des jederzeitigen Widerrufs [8], [9].
- Zur Datenverarbeitung müssen Privatpersonen ihr Alter verifizieren, da das Mindestalter zur Einwilligung der Datenverarbeitung bei 13 Jahren liegt (nach Artikel 8), was jedoch zwischen EU-Mitgliedstaaten variieren kann. Da die EU-DSGVO eine Prüfpflicht des Alters vorsieht, ist die alleinige Angabe des Alters nicht ausreichend. Laut Artikel 12 sind Unternehmen dazu verpflichtet, den Grund der Datenverarbeitung wie auch die Speicherdauer und die Weitergabe an Dritte mitzuteilen. Der Nutzer kann die Löschung der Daten anfordern, falls er nicht möchte, dass das Unternehmen weiterhin unter diesen Bedingungen mit den Daten arbeitet [8], [9].
- Das Löschen unerwünschter Daten, die von einem Unternehmen gespeichert wurden, kann gefordert werden. Dadurch haben Unternehmen nicht mehr die alleinigen Rechte an den personenbezogenen Daten.

- Mit der neuen Verordnung wurde der Rechtsstreit unter Juristen beantwortet, ob es sich bei IP-Adressen um personenbezogene Daten handelt. Die Verordnung definiert, dass die Möglichkeit besteht, Informationen aus den IP-Adressen zu gewinnen und diese somit personenbezogen sind. Dies bezieht sich ebenfalls auf Cookies, weswegen die Verordnung auch Auswirkungen auf das Online-Marketing haben könnte [9]. Das bedeutet, dass Privatpersonen darüber informiert werden müssen, wenn Daten aus dem Internet über sie gesammelt und genutzt werden. Der Anwender bekommt beim Surfen durch das Internet eine gewisse Sicherheit, die ihm vorher nicht gewährleistet werden konnte.

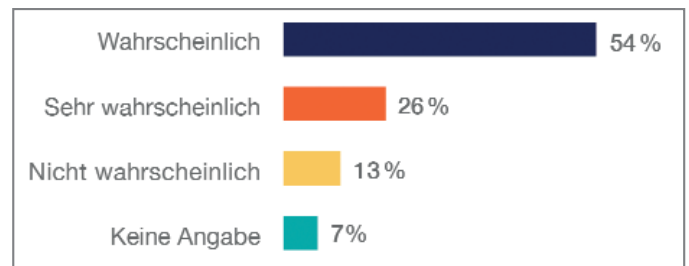
## Fazit

Durch die EU-DSGVO wurde Einiges an den Datenschutzregeln der EU-Mitgliedstaaten geändert. Während für Unternehmen bestehende Regeln ver-

schärft und neue Regeln ergänzt wurden, konnte für Verbraucher bzw. Privatpersonen die Erweiterung und Verstärkung der Rechte erreicht werden. Da der Datenschutz ein Grund-

rechtsschutz ist, umfasst dieser nur personenbezogene Daten. Durch den Erhalt eines Kündigungsschutzes profitiert die Berufsgruppe der Datenschutzbeauftragten von den Neuerungen in Deutschland. Das Ziel der EU-DSGVO ist demnach, die Sicherheit der Datenverarbeitung zu gewährleisten und „das Vertrauen in die Sicherheit von Transaktionen über das Internet herzustellen“ [11].

Unternehmen müssen sich bis Mai 2018 an die neue Verordnung anpassen. Dabei sollten sie sich u.a. folgende Fragen stellen [11]: Wer im Unternehmen braucht welche Daten wofür? Welche Daten müssen personen-



*Entsprechend einer internationalen Studie würde die Mehrheit der Befragten von dem neuen Gesetz Gebrauch machen (Quelle: Pegasystems)*

bezogen sein, welche können anonymisiert werden? Brauchen die Daten unnötigen Speicherplatz?

EU-Bürger können auch Dienstleistungen von internationalen Unternehmen in Anspruch nehmen, so dass betroffene Unternehmen an den europäischen Verbraucherschutz gebunden sind. Internationale Konzerne müssen sich an die Richtlinien des jeweiligen Mitgliedstaates halten und einen Vertreter für die EU benennen. Durch die neue Verordnung ändert sich dementsprechend einiges sowohl auf nationaler als auch auf internationaler Ebene – für Privatpersonen und Unternehmen. (bk)