

Neuerungen im EU-Datenschutz

Die letzten Monate brachten bedeutende Fortschritte im EU-Datenschutzregime. Nach knapp vierjährigen Verhandlungen steht das **neue „EU-Datenschutzpaket“** vor der Annahme. Europäische Nutzer sollen damit mehr Rechte und einen besseren Schutz ihrer persönlichen Daten erhalten. Gemeinsame europäische Datenschutzbestimmungen sind eine wesentliche Voraussetzung für die Verwirklichung des digitalen Binnenmarktes und bringen Erleichterungen und Ersparnisse für Unternehmen. Darüber hinaus soll der Datenschutz durch neue Regeln für die Übermittlung und Verarbeitung von **persönlichen Daten von EU-Bürgern in den USA** gestärkt werden.

Was ist das EU-Datenschutzpaket?

Derzeit gibt es eine Vielzahl von EU-Vorschriften zum Schutz personenbezogener Daten und zur Regelung des Datenverkehrs: Die **derzeit geltende Datenschutzrichtlinie (95/46/EG)**, die in jedem EU-Mitgliedstaat durch eigene Gesetze und mit unterschiedlichem Datenschutzniveau umgesetzt wurde, erfasst jede Datenverarbeitung, wurde aber 1995 und damit lange vor dem „digitalen Zeitalter“ erlassen. Verschiedene andere Rechtsakte sehen einzelne Vorschriften für jeweils spezifische Bereiche vor.

Um dieses Flickwerk zu beseitigen und moderne und EU-weit einheitliche Datenschutzvorschriften zu schaffen und gleichzeitig den freien Datenverkehr im Europäischen Binnenmarkt sicherzustellen, legte die Europäische Kommission (EK) 2012 das „EU-Datenschutzpaket“ vor. Es besteht aus zwei Rechtsakten, über welche Ende 2015 eine vorläufige politische Einigung zwischen Rat und Europäischem Parlament (EP) erzielt wurde:

- **Datenschutz-Grundverordnung:** Mit der Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr soll das allgemeine Datenschutzrecht EU-weit geregelt und die derzeit gültige Datenschutzrichtlinie ersetzt werden.
- **Datenschutz-RL:** Die vorgeschlagene 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 soll frühere Rahmenbeschlüsse ersetzen.

Was haben EU-Bürger von der Umsetzung des Datenschutzpakets?

Mit der Datenschutz-Grundverordnung wird erstmals **europaweit unmittelbar anwendbares Datenschutzrecht** geschaffen: Das bedeutet, dass die gleichen Regelungen in allen EU-Mitgliedstaaten gelten und zu vollziehen sind, so dass ein einheitlicher Rechtsrahmen für alle Bürger, Unternehmen und Behörden entsteht.

Unternehmen mit Sitz außerhalb Europas müssen dieselben Regeln befolgen, wenn sie Dienstleistungen in der EU anbieten.

- Die neuen Vorschriften stärken die bestehenden Rechte und geben den Bürgern mehr Kontrolle über ihre Daten. So dürfen Unternehmen sensible persönliche Daten erst nach dem **ausdrücklichen Einverständnis der Nutzer** verarbeiten und müssen die zuständigen nationalen Datenschutzbehörden so schnell wie möglich über **Verstöße gegen den Datenschutz informieren** (etwa wenn persönliche Daten gehackt worden sind). Nutzer müssen sich bei Beschwerden in Zukunft nicht mehr an den jeweiligen EU-Sitz des Unternehmens wenden, sondern sollen eine **nationale Anlaufstelle** aufsuchen können.
- Auch das „**Recht auf Vergessenwerden**“ wird erstmals gesetzlich verankert: Wenn ein EU-Bürger nicht mehr länger die Verarbeitung seiner veröffentlichten Daten wünscht und keine legitimen Gründe für deren Aufbewahrung vorliegen, müssen diese Daten von den Unternehmen bzw. Behörden gelöscht und damit für die Internetöffentlichkeit unsichtbar werden.
- Darüber hinaus enthält die Datenschutz-Grundverordnung Regelungen für die modernen Formen der Datenverarbeitung, etwa **Apps** und **soziale Netzwerke**: So soll etwa durch datenschutzfreundliche Voreinstellungen sowie Anonymisierung und Pseudonymisierung von Daten das Recht auf Datenschutz besser gewährleistet werden.
- Im Fall der Missachtung der neuen Datenschutzvorgaben drohen **Strafen in Höhe von bis zu vier Prozent des Jahresumsatzes** eines Unternehmens. Für große Konzerne wie Google oder Facebook wären dies Strafen in Milliardenhöhe.

Wie wird die digitale Wirtschaft durch die Datenschutz-Grundverordnung gestärkt?

- Durch die Vereinheitlichung der europäischen Datenschutznormen werden der grenzüberschreitende Dienstleistungs- und Warenverkehr erleichtert und Kosten gespart. Während die derzeit gültige Datenschutz-RL in den 28 EU-Mitgliedstaaten unterschiedlich umgesetzt wird, wird mit der neuen Datenschutz-Grundverordnung eine einheitliche Rechtsgrundlage geschaffen, die **in allen EU-Mitgliedstaaten die gleichen Rechte und Pflichten für Unternehmer und Bürger** vorsieht.
- Eine weitere Erleichterung ist, dass datenverarbeitende Unternehmen künftig EU-weit nur noch mit einer **einzigsten Aufsichtsbehörde** zu tun haben. Schätzungen zufolge werden dadurch Kosten in Höhe von etwa 2,3 Mrd. EUR jährlich eingespart.
- Mit den neuen Regeln wird statt einer aufwändigen allgemeingültigen Verpflichtung eine den jeweiligen Risiken angepasste Verpflichtung („**risikobasierter Ansatz**“) eingeführt: Je mehr Datenverarbeitungen in einem Unternehmen anfallen und je höher die Risiken für die Rechte und Freiheiten jener Personen, die von der Datenverarbeitung betroffenen scheinen, desto mehr Pflichten treffen das Unternehmen.

Welches Ziel verfolgt die neue Datenschutz-Richtlinie?

- Mit der Richtlinie für den **Datenschutz bei Polizei und Strafjustiz** werden personenbezogene Daten besser geschützt, wenn sie zum Zweck der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten verarbeitet werden – dies gilt für Daten von **Opfern, Zeugen und Verdächtigen** gleichermaßen.
- Die Datenschutz-RL enthält zudem auch klare **Regeln für den Transfer** personenbezogener Daten aus der EU hinaus, um zu gewährleisten, dass der in der EU dem Einzelnen garantierte Datenschutz nicht ausgehöhlt wird.
- Mit der Richtlinie werden die Strafverfolgungsbehörden in den EU-Mitgliedstaaten auch ermittlungsrelevante Informationen effizienter und wirksamer austauschen und bei der Bekämpfung von Terrorismus und sonstiger schwerer Kriminalität in Europa besser zusammenarbeiten können.
- Anders als die Datenschutz-Grundverordnung ist die Datenschutz-RL nur eine harmonisierte Grundlage und legt Mindestanforderungen für nationale Gesetze fest.

Warum wird das EU-Datenschutzpaket von Datenschützern kritisiert?

- Kritiker monieren, dass die Datenschutz-Grundverordnung unklare Formulierungen enthält, die bei Unternehmen zu Rechtsunsicherheit führen könnten. Es wird erwartet, dass einige Punkte erst durch den Europäischen Gerichtshof geklärt werden.
- Außerdem wird kritisiert, dass die Grundverordnung hinter den Anforderungen mancher nationaler Datenschutzregelungen, die derzeit schon gelten, zurückbleibt und durch nationale Gesetze ergänzt werden muss. Das könnte erneut zu einer Zersplitterung im EU-Datenschutzregime führen.

Wann werden die neue Datenschutz-Grundverordnung und -Richtlinie in Kraft treten?

Über das neue Datenschutzpaket wurde Mitte Dezember 2015 eine vorläufige politische Einigung erzielt, d.h. die EU-Gesetzgebungsorgane EK, Rat und EP haben sich in den Trilogverhandlungen auf die Gesetzestexte geeinigt. In den nächsten Wochen müssen nun das EP und der Rat die finalen Versionen noch förmlich annehmen. Anwendbar sollen die neuen Regeln dann zwei Jahre nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union, also voraussichtlich **Mitte 2018** sein.

Welche neuen Vereinbarungen im Datenschutzbereich gibt es mit den USA?

Die EK hat in den letzten Monaten mit der US-Regierung über zwei verschiedene Vereinbarungen im Datenschutzbereich verhandelt:

- 1) Das neue **EU-US-Datenschutzrahmenabkommen** („Umbrella Agreement“), das hohe Datenschutzstandards für der Strafverfolgung dienende Datenübermittlungen gewährleistet. Es soll auf sämtliche personenbezogenen Daten (z.B. Namen, Adressen,

Vorstrafenregister), die zur Vorbeugung, Aufdeckung, Ermittlung und Verfolgung von Straftaten, inklusive Terrorismus, zwischen der EU und den USA ausgetauscht werden, Anwendung finden.

- 2) Den **EU-US-Datenschutzschild („EU-US Privacy Shield“)**, ein Rahmen für den Austausch kommerzieller Daten. Dieses sieht Datenschutzbestimmungen für die Übertragung von persönlichen Daten v.a. durch Unternehmen in die USA und deren weitere Verarbeitung vor. Anfang Februar 2016 hat die EK den Abschluss der Verhandlungen bekannt gegeben.

Was bringt das EU-US-Datenschutzrahmenabkommen den BürgerInnen?

Bislang hatten EU-Bürger keine Möglichkeit, sich gerichtlich zur Wehr zu setzen, wenn US-Behörden ihnen Zugang zu den sie betreffenden persönlichen Daten oder deren Berichtigung verweigern oder diese unrechtmäßig preisgeben. Dies soll sich durch das neue Rahmenabkommen ändern: Neben einem **Gerichtsweg** sieht das Rahmenabkommen u.a. vor, dass persönliche Daten von US-Behörden **nur zur Vorbeugung, Aufdeckung, Ermittlung und Verfolgung von Straftaten** verwendet und nicht zu anderen Zwecken verarbeitet werden dürfen. Zudem sollen **Dauer der Aufbewahrung** und **Weiterübermittlung von Daten** klaren Grenzen unterliegen und jede Person ein **Recht auf Zugang** zu den sie betreffenden Daten – unter bestimmten Voraussetzungen und abhängig von den Erfordernissen der Strafverfolgung – und auf **Berichtigung unzutreffender Angaben** haben.

Was sind die weiteren Schritte?

Nachdem nunmehr der **Judicial Redress Act** von US Präsident Obama am 24.2.2016 unterzeichnet wurde, ein US Gesetz, das EU-Bürgern Zugang zu US-Gerichten bei Datenschutzverletzungen einräumt, kündigte die EK an, in Kürze die Unterzeichnung des Datenschutz-Rahmenabkommens vorzuschlagen. Über den Abschluss des Abkommens entscheidet der Rat nach Zustimmung des EP.

Warum war eine Nachfolgeregelung für das „Safe-Harbor-Abkommen“ notwendig?

Nach der oben erwähnten derzeit noch gültigen Datenschutzrichtlinie ist die Übermittlung von persönlichen Daten im Wirtschaftsverkehr in Nicht-EU-Staaten nur dann zulässig, wenn dort ein **„angemessenes Schutzniveau“** gewährleistet ist. Bisher war die Datenübertragung aus der EU in die USA im sog. **„Safe Harbor Abkommen“** geregelt. Der EuGH hatte jedoch in seiner Entscheidung vom 6. Oktober 2015 in Folge einer Beschwerde des österr. Jusstudenten Max Schrems gegen Facebook die Übertragung von Daten in die USA auf der Grundlage des „Safe-Harbour-Abkommens“ für unzulässig erklärt. Schrems hatte geltend gemacht, dass persönliche Daten in den USA nicht vor staatlicher Überwachung geschützt seien.

Mit dem **EU-US Privacy Shield** wird daher nunmehr eine **Nachfolgeregelung** für das „Safe-Harbor-Abkommen“ geschaffen. Dieses trägt den Datenschutzanforderungen der EU mit folgenden Zusicherungen von Seiten der USA Rechnung:

- Die US-Regierung soll nun erstmals schriftliche Zusicherungen vorlegen, dass der **Zugang von US-Strafverfolgungs- und Sicherheitsbehörden zu persönlichen Daten** klaren Regeln, **Grenzen und Kontrollen** unterliegen wird.
- Zudem müssen US-Unternehmen, die persönliche Daten aus Europa in die USA importieren, nach US-Recht durchsetzbare Verpflichtungserklärungen zur Begrenzung und Überwachung der Datenverarbeitung abgeben und veröffentlichen sowie auf **Beschwerden von EU-Bürgern über unrechtmäßige Datenweitergabe innerhalb einer gewissen Frist antworten**.
- Europäische Datenschutzbehörden können zudem **Beschwerden von EU-Bürgern dem US-Handelsministerium und der Wettbewerbsbehörde** weiterleiten.
- Eine neu geschaffene **Ombudsperson** wird für Beschwerden über unerlaubte Dateneingriffe durch US-Behörden zuständig sein.
- Die EK wird in Zukunft auch jährlich die **Einhaltung der Vereinbarungen mit der US-Regierung evaluieren** und darüber berichten.

Die US-Regierung hat die vereinbarten schriftlichen Zusicherungen Ende Februar vorgelegt. In der Folge hat auch die EK den ersten Entwurf einer neuerlichen Entscheidung, welche die Datenübertragungen in die USA für zulässig erklärt, veröffentlicht. An der Finalisierung dieses „Angemessenheitsbeschlusses“ wird derzeit unter Einbindung von Vertretern der Mitgliedsstaaten und der nationalen Datenschutzbehörden gearbeitet. Die EK plant, dass das EU-US Privacy Shield **bis Juni umgesetzt** wird.

Kritiker des neuen Abkommens geben zu bedenken, dass den US-Behörden nach wie vor zu viel Spielraum eingeräumt wird und dass die versprochenen Datenschutzvorkehrungen für persönliche Daten von EU-Bürgern in den USA nicht gesetzlich verankert werden.