von **Dr. Sebastian Kraska**

Datenschutz: Auswirkungen der EU-Datenschutzgrundverordnung

Mit der neuen EU-Datenschutzgrundverordnung (DSGVO-E) soll das europäische Datenschutzrecht vereinheitlicht werden. Die nach derzeitigem Planungsstand (bei noch ausstehender Zustimmung des EU-Parlaments) im ersten Quartal 2018 in Kraft tretende Neuregelung löst das bisherige Konzept einer europäischen Datenschutzrichtlinie (diese legte bislang die datenschutzrechtlichen Grundprinzipien fest) und darauf aufbauender einzelstaatlicher Datenschutzregelungen ab und ersetzt dies durch eine in allen EU-Mitgliedsstaaten direkt geltende EU-Datenschutzgrundverordnung (DSGVO-E).

Bericht von Herrn **Rechtsanwalt Dr. Sebastian Kraska**, **externer Datenschutzbeauftragter**.

Datenschutz-Grundprinzipen im Kern beibehalten

Die EU-Datenschutzgrundverordnung (DSGVO-E) schreibt im Kern die bisherigen datenschutzrechtlichen Grundprinzipien fort. Die Grundsätze der "Datenvermeidung und Datensparsamkeit", der "Zweckbindung", des "Verbots mit Erlaubnisvorbehalts" und der "Transparenz" finden sich auch im neuen Regelungskonzept wieder (vgl. vertiefend Artikel 5 "Principles relating to personal data processing" der neuen EU-Datenschutzgrundverordnung DSGVO-E).

Insbesondere um das "Verbot mit Erlaubnisvorbehalt" war zuletzt stark gestritten worden (nun festgeschrieben in Artikel 6 "Lawfulness of processing" der neuen EU-Datenschutzgrundverordnung DSGVO-E). Danach sind Datenverarbeitungsvorgänge nur zulässig, wenn die Person zugestimmt hat oder die Datenverarbeitung zur Vertragserfüllung erforderlich ist oder alternativ eine andere in der Vorschrift genannte Ausnahme eingreift. Dieser Regelungsansatz limitiert gerade Anwendungen und Auswertungsmöglichkeiten im Big Data-Bereich. Hier wird sich die Praxis noch stärker als bislang um den Einbau datenschutzfreundlicher Verarbeitungstechniken kümmern müssen (vgl. auch Artikel 23 "Data protection by design and by default" der neuen EU-Datenschutzgrundverordnung DSGVO-E).

Auswirkungen für produzierende Unternehmen

Für produzierende Unternehmen in Deutschland werden die Auswirkungen der EU-Datenschutzgrundverordnung DSGVO-E überschaubar bleiben (wenngleich die Regelungslage an Komplexität gewinnt und daher zumindest zu Beginn ein erhöhter Aufwand für die Umstellung auf die neuen rechtlichen Vorgaben zu erwarten ist). Bislang bereits aus dem Bundesdatenschutzgesetz bekannte Mindest-Standards für die betriebliche Praxis werden im Wesentlichen fortgeführt:

- Werden Datenverarbeitungsvorgänge ausgelagert müssen die Details in einem begleitenden Auftragsdatenverarbeitungsvertrag festgehalten werden (Artikel 26 "Processor" der neuen EU-Datenschutzgrundverordnung DSGVO-E)
- Zentrale Verfahren müssen schriftlich dokumentiert werden (Artikel 28 "Records of processing activities" der neuen EU-Datenschutzgrundverordnung DSGVO-E)
- Unternehmen müssen einen Datenschutzbeauftragten bestellen (die neue EU-Datenschutzgrundverordnung DSGVO-E sieht eine Bestellverpflichtung vor, wenn der Focus der Tätigkeit auf der Datenverarbeitung liegt oder wenn Mitgliedstaaten zusätzlich eine Bestellpflicht vorsehen) (Artikel 35 "Designation of the data protection officer" der neuen EU-Datenschutzgrundverordnung DSGVO-E)
- Die mit der Datenverarbeitung befassten Beschäftigten sind im Datenschutz durch den Datenschutzbeauftragten zu schulen (Artikel 37 "Tasks of the data protection officer" der neuen EU-Datenschutzgrundverordnung DSGVO-E)
- Das Unternehmen hat ausreichende Ressourcen für eine dem Stand der Technik entsprechende IT-Landschaft zur Verfügung zu stellen (Artikel 30 "Security of processing" der neuen EU-Datenschutzgrundverordnung DSGVO-E)
- Im Fall von bestimmten Datenverlustszenarien müssen die Betroffenen sowie die Datenschutz-Aufsichtsbehörden informiert werden (Artikel 31 "Notification of a personal data breach to the supervisory authority" und Artikel 32 "Communication of a personal data breach to the data subject" der neuen EU-Datenschutzgrundverordnung DSGVO-E)

Verhältnis zum nationalen Recht

Die Diskussion der kommenden Jahre wird auch die Frage des Verhältnisses zum nationalen Recht begleiten.

So sieht die Verordnung an einer ganzen Reihe zentraler Regelungspunkte die Möglichkeit vor, durch nationales Recht Sonderregelungen zu schaffen. Auch die EU-Datenschutzgrundverordnung DSGVO-E wird daher das Datenschutzrecht in der Europäischen Union nicht vollständig harmonisieren. Dieser Kompromiss war zuletzt in den Trilog-Verhandlungen insbesondere mit dem EU-Rat notwendig geworden, der in großem Umfang entsprechende Abweichungsmöglichkeiten in die Verhandlungen eingebracht hatte (die vorliegende EU-Datenschutzgrundverordnung DSGVO-E ist eher ein Rechtskonstrukt zwischen Richtlinie und Verordnung).

Bei einer Reihe von Themen sind nationale Abweichungen möglich, wobei zusätzlich die Frage derzeit noch offen ist, wie sich die Anwendbarkeit der nationalen Regelungen auf Basis oder parallel zur EU-Datenschutzgrundverordnung DSGVO-E bestimmen wird.

Im Folgenden finden Sie eine durch uns erstellte Auswahl der Abweichungsmöglichkeiten:

1. Details zur Definition der "verantwortlichen Stelle" (Artikel 4 (5) "Definitions" und Artikel 24 "Joint controllers" der neuen EU-Datenschutzgrundverordnung DSGVO-E)

2. Details zur Definition des "Empfängers" (Artikel 4 (7) "Definitions" der neuen EU-Datenschutzgrundverordnung DSGVO-E)

3. Ausgestaltung gesonderter nationaler Erlaubnistatbestände zur Verarbeitung personenbezogener Daten (Artikel 6 (2a) "Lawfulness of processing" der neuen EU-Datenschutzgrundverordnung DSGVO-E)

4. Absenkung der Altersgrenzer zur Einwilligung durch Kinder auf bis zu 13 Jahre (Artikel 8 (1) "Conditions applicable to child's consent in relation to information society services" der neuen EU-Datenschutzgrundverordnung DSGVO-E)

5. Ausgestaltung gesonderter nationaler Erlaubnistatbestände zur Verarbeitung besonderer Arten personenbezogener Daten (Artikel 9 (2) (4) (5) "Processing of special categories of personal data" der neuen EU-Datenschutzgrundverordnung DSGVO-E)

6. Nationale Spezialregelung/Einschränkung der Informationsansprüche des Betroffenen (Artikel 14a (4c) (4d) "Information to be provided where the data have not been obtained from the data subject" der neuen EU-Datenschutzgrundverordnung DSGVO-E)

7. Einschränkung des Rechts auf Datenlöschung des Betroffenen (Artikel 17 (3b) "Right to erasure ("right to be forgotten")" der neuen EU-Datenschutzgrundverordnung DSGVO-E)

8. Einschränkung des Verbots der automatisierten Einzelentscheidungen (Artikel 20 (1a b) "Automated individual decision making, including profiling" der neuen EU-Datenschutzgrundverordnung DSGVO-E)

9. Anwendungseinschränkungen sämtlicher Betroffenenrechte (nach den Artikeln 12 bis 20) einschließlich der Datenschutzgrundprinzipien (Artikel 5) und der Informationspflicht im Datenverlustfall (Artikel 32) (Artikel 21 "Restrictions" der neuen EU-Datenschutzgrundverordnung DSGVO-E)

10. Schaffung nationaler Datenverarbeitungsvorgaben für Auftragsdatenverarbeitungsnehmer (Artikel 27 "Processing under the authority of the controller and processor" und Artikel 30 (2b) der neuen EU-Datenschutzgrundverordnung DSGVO-E)

11. Verschärfung zur Durchführung von Vorabkontrollverfahren für neue datenverarbeitende Systeme (Artikel 33 (5) "Processing under the authority of the controller and processor" der neuen EU-Datenschutzgrundverordnung DSGVO-E)

12. Erweiterung der Bestell-Voraussetzungen eines Datenschutzbeauftragten (Artikel 35 (4) "Designation of the data protection officer" der neuen EU-Datenschutzgrundverordnung DSGVO-E)

13. Erleichterung von Datentransfers an Stellen außerhalb der europäischen Union (Artikel 44 "Derogations for specific situations" der neuen EU-Datenschutzgrundverordnung DSGVO-E)

14. Schaffung von nationalen Ausnahmen von Regelungsgrundsätzen bei Datenverarbeitungsvorgängen für journalistische Zwecke (Artikel 80 "Processing of personal data and freedom of expression and information" der neuen EU-Datenschutzgrundverordnung DSGVO-E)

15. Spezifische Ausgestaltung bei Verwendung einer nationalen Identifizierungsnummer (Artikel 80b "Processing of national identification number" der neuen EU-Datenschutzgrundverordnung DSGVO-E)

16. Schaffung nationale Spezialregelungen bei der Verarbeitung von Beschäftigtendaten (Artikel 82 "Processing in the employment context" der neuen EU-Datenschutzgrundverordnung DSGVO-E)

17. Schaffung von nationalen Ausnahmen von Regelungsgrundsätzen bei Datenverarbeitungsvorgängen für archivarische Zwecke (Artikel 83 "Safeguards and derogations for the processing of personal data for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes" der neuen EU-Datenschutzgrundverordnung DSGVO-E)

18. Schaffung besonderer nationaler Geheimhaltungsverpflichtungen (Artikel 84 " Obligations of secrecy" der neuen EU-Datenschutzgrundverordnung DSGVO-E)

Zum anderen wird in Deutschland möglicherweise die Frage aufgeworfen werden, in welchem Verhältnis die EU-Datenschutzgrundverordnung DSGVO-E zu den vom Bundesverfassungsrecht im Recht auf informationelle Selbstbestimmung festgehaltenen Grundrecht steht und ob die verfassungsrechtlichen Vorgaben insoweit ausreichend Beachtung gefunden haben.

Ebenfalls diskussionswürdig erscheint die Frage, ob ein ursprünglich im Kern als Abwehrrecht des Einzelnen gegen staatliche Datensammlung gedachtes Verfassungsrecht nun in eine auf reine Regulierung privatwirtschaftlicher Datenverarbeitung zielende Regelung verfassungskonform münden kann.

Angesichts der Komplexität der EU-Datenschutzgrundverordnung DSGVO-E steht auch die Frage im Raum, ob diese das verfassungsrechtlich geforderte Mindestmaß an Rechtssicherheit (insb. Rechtsklarheit) erfüllt.

Änderungen insbesondere für datengetriebene Unternehmen und Konzerne

Relevante Anpassungen ergeben sich insbesondere für datengetriebene Unternehmen. So werden insbesondere die folgenden regulativen Anpassungen zu berücksichtigen sein:

- Das bisher in der EU-Datenschutzrichtlinie geltende (und zuletzt vom EuGH bereits deutlich abgeschwächte) Territorialitätsprinzip wird im Ergebnis durch ein Marktortprinzip ersetzt. Richtet sich ein Angebot damit an einen bestimmten nationalen Markt unterliegt dies damit auch der nationalen Datenschutz-Aufsicht (Artikel 4 (19a b) "Definitions" der neuen EU-Datenschutzgrundverordnung DSGVO-E).
- Die Voraussetzungen zur Verarbeitung personenbezogener Daten werden häufig auf "berechtigte Interessen" gestützt werden können und damit in der Tendenz eher gesenkt (vgl. Härting in "Reasonable expectations of privacy": [Wie sich die DSGVO dem US-Recht annähert](http://www.cr-online.de/blog/2015/12/18/reasonable-expectations-of-privacy-wie-sich-die-dsgvo-dem-us-recht-annaehert); dies gilt in gleicher Weise für die Datenverarbeitung im Konzern, die dadurch erleichtert wird.
- Die Tätigkeit der Datenschutz-Aufsichtsbehörden soll harmonisiert werden. Durch die Schaffung eines "European Data Protection Board" soll eine einheitliche Stelle zur Auslegung des europäischen Datenschutzrechts geschaffen werden (Artikel 58 "Opinion by the European Data Protection Board" der neuen EU-Datenschutzgrundverordnung DSGVO-E)
- Der Bußgeldrahmen wird drastisch erhöht. Im Extremfall können bis zu 4 % des weltweiten Jahresumsatzes gefordert werden. Eine Strafzahlung die in dieser Höhe in der Praxis mangels Angemessenheit vermutlich eher selten zur Anwendung kommen dürfte, in der öffentlichen Diskussion

aber für hohe Aufmerksamkeit gesorgt hat (Artikel 79 (3a) "General conditions for imposing administrative fines" der neuen EU-Datenschutzgrundverordnung DSGVO-E).

- Schaffung einer europaweiten Verpflichtung zur Bestellung eines Datenschutzbeauftragten, wenn das Geschäftsmodell im Kern auf der Verarbeitung personenbezogener Daten beruht oder nationale Vorgaben zusätzliche Bestellpflichten konstituieren (Artikel 35 "Designation of the data protection officer" der neuen EU-Datenschutzgrundverordnung DSGVO-E).
- Bei Verarbeitung von Daten im Auftrag wird der Auftragsdatenverarbeitungsnehmer ("Processor"), stärker als bislang nach dem Bundesdatenschutzgesetz der Fall, in die datenschutzrechtliche Verantwortung genommen (z.B. Artikel 30 "Security of processing" der neuen EU-Datenschutzgrundverordnung DSGVO-E; Artikel 79 "General conditions for imposing administrative fines" der neuen EU-Datenschutzgrundverordnung DSGVO-E).
- Schaffung legislativer Vorgaben für Datenschutz-Zertifizierungen auf europäischer Ebene (Artikel 39 "Certification" der neuen EU-Datenschutzgrundverordnung DSGVO-E) und die Verpflichtung, datenschutzfreundliche Technik bereits zu Beginn zu implementieren Artikel 23 "Data protection by design and by default" der neuen EU-Datenschutzgrundverordnung DSGVO-E).

Strukturierung des weiteren Vorgehens

Unternehmen sind gehalten, die Zeit bis zum Inkrafttreten des neuen europäischen Datenschutzrechts im Jahr 2018 zu nutzen, die eigenen Datenverarbeitungsprozesse auf Anpassungsbedarf zu überprüfen. Bei der Neueinführung von Systemen sollten zudem gleich die neuen EU-Datenschutzregelungen soweit möglich mit berücksichtigt werden.

Bei weiteren Fragen zum Thema Datenschutz im Unternehmen wenden Sie sich bitte direkt an Herrn Dr. Kraska (erreichbar per Telefon unter 089-18 91 73 60 oder per E-Mail unter email@iitr.de).

Kontakt: IITR Institut für IT-Recht - IITR GmbH
Externer Datenschutzbeauftragter
Telefon: 089-18 91 73 60
E-Mail: email@iitr.de

Das Institut für IT-Recht berät Unternehmen bei der Bewältigung datenschutzrechtlicher Anforderungen. Zur Förderung wissenschaftlicher Angelegenheiten wird das Institut von einem wissenschaftlichen Beirat unterstützt. Auf www.iitr.de finden Sie regelmäßig neue Beiträge zu Fragen des Datenschutzrechts.

Autor:
Dr. Sebastian Kraska
Rechtsanwalt